



Wireless LAN Mobility System

Wireless LAN Switch and Controller Command Reference

WX4400	3CRWX440095A
WX2200	3CRWX220095A
WX1200	3CRWX120695A
WXR100	3CRWXR10095A

<http://www.3Com.com/>

Part No. 10015910 Rev AB
Published December 2007



3Com Corporation
350 Campus Drive
Marlborough, MA USA
01752-3064

Copyright © 2007, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com is a registered trademark of 3Com Corporation. The 3Com logo is a trademark of 3Com Corporation.

Mobility Domain, Managed Access Point, Mobility Profile, Mobility System, Mobility System Software, MP, MSS, and SentrySweep are trademarks of Trapeze Networks.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, Windows XP, and Windows NT are registered trademarks of Microsoft Corporation.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

CONTENTS

ABOUT THIS GUIDE

- Conventions 23
- Documentation 24
- Documentation Comments 25

1 USING THE COMMAND-LINE INTERFACE

- Overview 27
- CLI Conventions 28
 - Command Prompts 28
 - Syntax Notation 28
 - Text Entry Conventions and Allowed Characters 29
 - MAC Address Notation 29
 - IP Address and Mask Notation 30
 - User Globs, MAC Address Globs, and VLAN Globs 30
 - Port Lists 32
 - Virtual LAN Identification 33
- Command-Line Editing 33
 - Keyboard Shortcuts 33
 - History Buffer 34
 - Tabs 34
 - Single-Asterisk (*) Wildcard Character 34
 - Double-Asterisk (**) Wildcard Characters 34
- Using CLI Help 35
- Understanding Command Descriptions 36

2 ACCESS COMMANDS

- Commands by Usage 37
 - disable 37
 - enable 38
 - quit 38
 - set enablepass 39

3 SYSTEM SERVICE COMMANDS

Commands by Usage	41
clear banner motd	42
clear history	43
clear prompt	43
clear system	44
display banner motd	45
display base-information	45
display license	46
display load	47
display system	47
help	50
history	51
quickstart	52
set auto-config	52
set banner acknowledge	54
set banner motd	56
set confirm	57
set length	57
set license	58
set prompt	59
set system contact	60
set system countrycode	61
set system idle-timeout	65
set system ip-address	66
set system location	67
set system name	68

4 PORT COMMANDS

Commands by Usage	69
clear ap	70
clear port counters	71
clear port-group	71
clear port media-type	72
clear port name	72
clear port mirror	73
clear port preference	73

clear port type 74
display port counters 75
display port-group 76
display port mirror 77
display port poe 78
display port status 79
display port media-type 81
monitor port counters 82
reset port 87
set ap 87
set port 89
set port-group 90
set port media-type 91
set port mirror 92
set port name 93
set port negotiation 93
set port poe 94
set port speed 95
set port trap 96
set port type ap 97
set port type wired-auth 100

5 VLAN COMMANDS

Commands by usage 103
clear fdb 104
clear security 12-restrict 105
clear security 12-restrict counters 106
clear vlan 107
clear vlan-profile 108
display fdb 109
display fdb agingtime 111
display fdb count 112
display roaming station 113
display roaming vlan 115
display security 12-restrict 116
display tunnel 117
display vlan config 118

display vlan-profile 120
set fdb 121
set fdb agingtime 122
set security l2-restrict 123
set vlan name 124
set vlan port 125
set vlan tunnel-affinity 126
set vlan profile 127

6 QUALITY OF SERVICE COMMANDS

Commands by Usage 129
clear qos 129
set qos cos-to-dscp-map 131
set qos dscp-to-cos-map 132
display qos 133
display qos dscp-table 134

7 IP SERVICES COMMANDS

Commands by Usage 135
clear interface 137
clear ip alias 138
clear ip dns domain 139
clear ip dns server 139
clear ip route 140
clear ip telnet 141
clear ntp server 141
clear ntp update-interval 142
clear snmp community 143
clear snmp notify profile 143
clear snmp notify target 144
clear snmp usm 144
clear summertime 145
clear system ip-address 146
clear timezone 146
display arp 147
display dhcp-client 148
display dhcp-server 150

display interface 152
display ip alias 153
display ip dns 154
display ip https 155
display ip route 156
display ip telnet 158
display ntp 159
display snmp community 161
display snmp counters 162
display snmp notify profile 162
display snmp notify target 162
display snmp status 163
display snmp usm 164
display summertime 164
display timedate 165
display timezone 165
ping 166
set arp 168
set arp agingtime 169
set interface 170
set interface dhcp-client 171
set interface dhcp-server 172
set interface status 173
set ip alias 174
set ip dns 175
set ip dns domain 175
set ip dns server 176
set ip https server 177
set ip route 178
set ip snmp server 180
set ip ssh 180
set ip ssh server 181
set ip telnet 181
set ip telnet server 182
set ntp 183
set ntp server 184
set ntp update-interval 185
set snmp community 185

set snmp notify profile 187
set snmp notify target 192
 SNMPv3 with Informs 192
 SNMPv3 with Traps 193
 SNMPv2c with Informs 194
 SNMPv2c with Traps 195
 SNMPv1 with Traps 195
set snmp protocol 197
set snmp security 198
set snmp usm 199
set summertime 202
set system ip-address 203
set timedate 204
set timezone 205
telnet 206
traceroute 207

8 AAA COMMANDS

Commands by Usage 211
clear accounting 213
clear authentication admin 214
clear authentication console 215
clear authentication dot1x 216
clear authentication mac 217
clear authentication proxy 218
clear authentication web 218
clear location policy 219
clear mac-user 220
clear mac-user attr 221
clear mac-user group 221
clear mac-usergroup 222
clear mac-usergroup attr 223
clear mobility-profile 224
clear user 224
clear user attr 225
clear user group 226
clear user lockout 226

clear usergroup 227
clear usergroup attr 228
display aaa 229
display accounting statistics 232
display location policy 234
display mobility-profile 235
set accounting {admin | console} 235
set accounting {dot1x | mac | web | last-resort} 237
set authentication admin 239
set authentication console 241
set authentication dot1x 243
set authentication mac 247
set authentication max-attempts 249
set authentication max-attempts 250
set authentication minimum-password-length 251
set authentication password-restrict 252
set authentication proxy 253
set authentication web 254
set location policy 256
set mac-user 260
set mac-user attr 261
set mac-usergroup attr 267
set mobility-profile 269
set mobility-profile mode 271
set user 271
set user attr 273
set user expire-password-in 274
set user group 275
set usergroup 275
set usergroup expire-password-in 277
set web-portal 278

9 MOBILITY DOMAIN COMMANDS

Commands by Usage 279
clear mobility-domain 280
clear mobility-domain member 280
display mobility-domain 281

display mobility-domain config 282
display mobility-domain status 283
set mobility-domain member 284
set mobility-domain mode member secondary seed-ip 285
set mobility-domain mode member seed-ip 286
set mobility-domain mode secondary-seed domain-name 287
set mobility-domain mode seed domain-name 288
set domain security 289

10 NETWORK DOMAIN COMMANDS

Network Domain Commands by Usage 291
clear network-domain 292
clear network-domain mode 293
clear network-domain peer 294
clear network-domain seed-ip 295
display network-domain 296
set network-domain mode member seed-ip 298
set network-domain peer 299
set network-domain mode seed domain-name 300

11 MANAGED ACCESS POINT COMMANDS

MAP Access Point Commands by Usage 301
clear ap local-switching vlan-profile 307
clear ap radio 308
clear ap boot-configuration 310
clear ap radio load-balancing group 311
clear radio-profile 312
clear service-profile 313
display ap arp 314
display ap config 316
display ap counters 319
display ap fdb 325
display ap qos-stats 326
display ap etherstats 327
display ap group 329
display ap mesh-links 329
display ap status 331

display ap vlan 337
display auto-tune attributes 338
display auto-tune neighbors 340
display ap boot-configuration 342
display ap connection 343
display ap global 345
display ap unconfigured 347
display load-balancing group 348
display radio-profile 350
display service-profile 353
reset ap 362
set ap auto 362
set ap auto persistent 364
set ap auto radiotype 365
set ap auto mode 366
set ap bias 367
set ap blink 368
set ap boot-configuration ip 369
set ap boot-configuration mesh mode 370
set ap boot-configuration mesh psk-phrase 371
set ap boot-configuration mesh psk-raw 372
set ap boot-configuration mesh ssid 373
set ap boot-configuration switch 374
set ap boot-configuration vlan 375
set ap contact 376
set ap fingerprint 376
set ap force-image-download 378
set ap group 379
set ap location 379
set ap local-switching mode 379
set ap local-switching vlan-profile 380
set ap name 381
set ap radio antenna-location 382
set ap radio antenntype 383
set ap radio auto-tune max-power 384
set ap radio auto-tune max-retransmissions 385

set ap radio channel 387
set ap radio link-calibration 388
set ap radio load balancing 389
set ap radio load balancing group 390
set ap radio mode 391
set ap radio radio-profile 392
set ap radio tx-power 393
set ap security 395
set ap upgrade-firmware 396
set band-preference 397
set load-balancing mode 398
set load-balancing strictness 399
set radio-profile 11g-only 400
set radio-profile active-scan 400
set radio-profile auto-tune 11a-channel-range 401
set radio-profile auto-tune channel-config 402
set radio-profile auto-tune channel-holddown 403
set radio-profile auto-tune channel-interval 404
set radio-profile auto-tune channel-lockdown 405
set radio-profile auto-tune power-config 406
set radio-profile auto-tune power-interval 407
set radio-profile auto-tune power-lockdown 408
set radio-profile auto-tune power-ramp-interval 409
set radio-profile beacon-interval 409
set radio-profile countermeasures 410
set radio-profile dtim-interval 412
set radio-profile frag-threshold 413
set radio-profile long-retry 414
set radio-profile max-rx-lifetime 414
set radio-profile max-tx-lifetime 415
set radio-profile mode 416
set radio-profile preamble-length 419
set radio-profile qos-mode 420
set radio-profile rfid-mode 421
set radio-profile rate-enforcement 421
set radio-profile rts-threshold 423
set radio-profile service-profile 424
set radio-profile short-retry 430

set radio-profile wmm 430
set radio-profile wmm-powersave 430
set service-profile attr 431
set service-profile auth-dot1x 433
set service-profile auth-fallthru 434
set service-profile auth-psk 435
set service-profile beacon 436
set service-profile bridging 437
set service-profile cac-mode 438
set service-profile cac-session 439
set service-profile cipher-ccmp 440
set service-profile cipher-tkip 441
set service-profile cipher-wep104 442
set service-profile cipher-wep40 443
set service-profile cos 444
set service-profile dhcp-restrict 445
set service-profile idle-client-probing 446
set service-profile keep-initial-vlan 447
set service-profile load-balancing-exempt 448
set service-profile long-retry-count 449
set service-profile mesh 450
set service-profile no-broadcast 451
set service-profile proxy-arp 452
set service-profile psk-phrase 453
set service-profile psk-raw 454
set service-profile rsn-ie 455
set service-profile shared-key-auth 456
set service-profile short-retry-count 456
set service-profile soda agent-directory 457
set service-profile soda enforce-checks 458
set service-profile soda failure-page 459
set service-profile soda logout-page 460
set service-profile soda mode 462
set service-profile soda remediation-acl 463
set service-profile soda success-page 464
set service-profile ssid-name 465
set service-profile ssid-type 466

set service-profile tkip-mc-time 466
set service-profile static-cos 467
set service-profile transmit-rates 468
set service-profile use-client-dscp 470
set service-profile user-idle-timeout 471
set service-profile web-portal-acl 472
set service-profile web-portal-form 473
set service-profile web-portal-logout logout-url 475
set service-profile web-portal-logout mode 476
set service-profile web-portal-session-timeout 477
set service-profile wep active-multicast-index 478
set service-profile wep active-unicast-index 479
set service-profile wep key-index 480
set service-profile wpa-ie 481

12 STP COMMANDS

STP Commands by Usage 483
clear spantree portcost 484
clear spantree portpri 485
clear spantree portvlancost 485
clear spantree portvlanpri 486
clear spantree statistics 487
display spantree 488
display spantree backbonefast 491
display spantree blockedports 492
display spantree portfast 493
display spantree portvlancost 494
display spantree statistics 494
display spantree uplinkfast 500
set spantree 501
set spantree backbonefast 502
set spantree fwddelay 503
set spantree hello 503
set spantree maxage 504
set spantree portcost 505
set spantree portfast 506

set spantree portpri 507
set spantree portvlancost 508
set spantree portvlanpri 509
set spantree priority 510
set spantree uplinkfast 510

13 IGMP SNOOPING COMMANDS

Commands by usage 513
clear igmp statistics 514
display igmp 514
display igmp mrouter 518
display igmp querier 519
display igmp receiver-table 521
display igmp statistics 523
set igmp 525
set igmp lmqi 526
set igmp mrouter 527
set igmp mrsol 528
set igmp mrsol mrsi 528
set igmp oqi 529
set igmp proxy-report 530
set igmp qi 531
set igmp qri 532
set igmp querier 533
set igmp receiver 533
set igmp rv 534

14 SECURITY ACL COMMANDS

Security ACL Commands by Usage 537
clear security acl 538
clear security acl map 539
commit security acl 541
display security acl 542
display security acl editbuffer 543
display security acl hits 544
display security acl info 545
display security acl map 546

display security acl resource-usage 547
rollback security acl 551
set security acl 552
set security acl map 557
set security acl hit-sample-rate 559

15 CRYPTOGRAPHY COMMANDS

Commands by Usage 562
crypto ca-certificate 562
crypto certificate 564
crypto generate key 565
crypto generate request 566
crypto generate self-signed 568
crypto otp 570
crypto pkcs12 572
display crypto ca-certificate 573
display crypto certificate 574
display crypto key domain 576
display crypto key ssh 576

16 RADIUS AND SERVER GROUP COMMANDS

Commands by Usage 577
clear radius 578
clear radius client system-ip 579
clear radius proxy client 580
clear radius proxy port 580
clear radius server 581
clear server group 581
set radius 582
set radius client system-ip 584
set radius proxy client 585
set radius proxy port 586
set radius server 587
set server group 589
set server group load-balance 590

17 802.1X MANAGEMENT COMMANDS

Commands by Usage 593
clear dot1x bonded-period 594
clear dot1x max-req 595
clear dot1x port-control 595
clear dot1x quiet-period 596
clear dot1x reauth-max 597
clear dot1x reauth-period 597
clear dot1x timeout auth-server 598
clear dot1x timeout supplicant 598
clear dot1x tx-period 599
display dot1x 599
set dot1x authcontrol 602
set dot1x bonded-period 603
set dot1x key-tx 604
set dot1x max-req 605
set dot1x port-control 606
set dot1x quiet-period 607
set dot1x reauth 607
set dot1x reauth-max 608
set dot1x reauth-period 609
set dot1x timeout auth-server 609
set dot1x timeout supplicant 610
set dot1x tx-period 610
set dot1x wep-rekey 611
set dot1x wep-rekey-period 612

18 SESSION MANAGEMENT COMMANDS

Commands by Usage 613
clear sessions 613
clear sessions network 615
display sessions 616
display sessions mesh-ap 619
display sessions network 620

19 RF DETECTION COMMANDS

Commands by Usage 629
clear rfdetect attack-list 630
clear rfdetect black-list 631
clear rfdetect ignore 631
clear rfdetect ssid-list 632
clear rfdetect vendor-list 633
rfping 634
display rfdetect attack-list 635
display rfdetect black-list 636
display rfdetect clients 637
display rfdetect countermeasures 639
display rfdetect counters 640
display rfdetect data 642
display rfdetect ignore 644
display rfdetect mobility-domain 644
display rfdetect ssid-list 649
display rfdetect vendor-list 649
display rfdetect visible 650
set rfdetect active-scan 652
set rfdetect attack-list 653
set rfdetect black-list 654
set rf detect countermeasures 654
set rfdetect countermeasures mac 655
set rfdetect ignore 656
set rfdetect log 657
set rfdetect signature 658
set rfdetect signature key 659
set rfdetect ssid-list 659
set rfdetect vendor-list 660
test rflink 661

20 FILE MANAGEMENT COMMANDS

Commands by Usage 663
backup 664
clear boot backup-configuration 666
clear boot config 666

copy 667
delete 669
dir 670
install soda agent 673
display boot 674
display config 675
display version 677
load config 679
md5 681
mkdir 681
reset system 683
restore 684
rmdir 685
save config 685
set boot backup-configuration 686
set boot configuration-file 687
set boot partition 688
uninstall soda agent 688

21 TRACE COMMANDS

Commands by Usage 691
clear log trace 692
clear trace 692
display trace 693
save trace 694
set trace authentication 694
set trace authorization 695
set trace dot1x 696
set trace sm 697

22 SNOOP COMMANDS

Commands by Usage 699
clear snoop 700
clear snoop map 700
set snoop 701
set snoop map 704
set snoop mode 705

display snoop 706
display snoop info 706
display snoop map 707
display snoop stats 708

23 SYSTEM LOG COMMANDS

Commands by Usage 711
clear log 711
display log buffer 712
display log config 714
display log trace 715
set log 716
set log mark 719

24 BOOT PROMPT COMMANDS

Boot Prompt Commands by Usage 721
autoboot 722
boot 723
change 725
create 726
delete 727
dhcp 728
diag 729
dir 729
display 730
fver 732
help 733
ls 734
next 735
reset 736
test 737
version 738

A OBTAINING SUPPORT FOR YOUR 3COM PRODUCTS

Register Your Product to Gain Service Benefits 739
Solve Problems Online 739

Purchase Extended Warranty and Professional Services	740
Access Software Downloads	740
Contact Us	740
Telephone Technical Support and Repair	741

INDEX

ABOUT THIS GUIDE

This command reference explains Mobility System Software (MSS™) command line interface (CLI) that you enter on a 3Com WXR100 or WX1200 Wireless Switch or WX4400 or WX2200 Wireless LAN Controller to configure and manage the Mobility System™ wireless LAN (WLAN).

Read this reference if you are a network administrator responsible for managing WXR100, WX1200, WX4400, or WX2200 wireless switches and their Managed Access Points (MAPs) in a network.



If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the 3Com World Wide Web site:

<http://www.3com.com/>

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device

This manual uses the following text and syntax conventions:

Table 2 Text Conventions

Convention	Description
Monospace text	Sets off command syntax or sample commands and system responses.
Bold text	Highlights commands that you enter or items you select.
<i>Italic text</i>	Designates command variables that you replace with appropriate values, or highlights publication titles or words requiring special emphasis.
[] (square brackets)	Enclose optional parameters in command syntax.
{ } (curly brackets)	Enclose mandatory parameters in command syntax.
(vertical bar)	Separates mutually exclusive options in command syntax.
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in <i>italics</i>	Italics are used to: <ul style="list-style-type: none"> ■ Emphasize a point. ■ Denote a new term at the place where it is defined in the text. ■ Highlight an example string, such as a username or SSID.

Documentation

The MSS documentation set includes the following documents.

- *Wireless Switch Manager (3WXM) Release Notes*
These notes provide information about the 3WXM software release, including new features and bug fixes.
- *Wireless LAN Switch and Controller Release Notes*
These notes provide information about the MSS software release, including new features and bug fixes.
- *Wireless LAN Switch and Controller Quick Start Guide*
This guide provides instructions for performing basic setup of secure (802.1X) and guest (WebAAA™) access, for configuring a Mobility Domain for roaming, and for accessing a sample network plan in 3WXM for advanced configuration and management.

- [Wireless Switch Manager Reference Manual](#)

This manual shows you how to plan, configure, deploy, and manage a Mobility System wireless LAN (WLAN) using the 3Com Wireless Switch Manager (3WXM).
- [Wireless Switch Manager User's Guide](#)

This manual shows you how to plan, configure, deploy, and manage the entire WLAN with the 3WXM tool suite. Read this guide to learn how to plan wireless services, how to configure and deploy 3Com equipment to provide those services, and how to optimize and manage your WLAN.
- [Wireless LAN Switch and Controller Hardware Installation Guide](#)

This guide provides instructions and specifications for installing a WX wireless switch in a Mobility System WLAN.
- [Wireless LAN Switch and Controller Configuration Guide](#)

This guide provides instructions for configuring and managing the system through the Mobility System Software (MSS) CLI.
- [Wireless LAN Switch and Controller Command Reference](#)

This reference provides syntax information for all MSS commands supported on WX switches.

Documentation Comments

Your suggestions are very important to us. They will help make our documentation more useful to you. Please e-mail comments about this document to 3Com at:

pddtechpubs_comments@3com.com

Please include the following information when contacting us:

- *Document title*
- *Document part number and revision (on the title page)*
- *Page number (if appropriate)*

Example:

- *Wireless LAN Switch and Controller Configuration Guide*
- *Part number 730-9502-0071, Revision B*
- *Page 25*



Please note that we can only respond to comments and questions about 3Com product documentation at this e-mail address. Questions related to Technical Support or sales should be directed in the first instance to your network supplier.

1

USING THE COMMAND-LINE INTERFACE

This chapter discusses the 3Com Wireless Switch Manager (3WXM) command-line interface (CLI). Described are:

- CLI conventions (see “CLI Conventions” on page 28)
- Editing on the command line (see “Command-Line Editing” on page 33)
- Using the CLI help feature (see “Using CLI Help” on page 35)
- Information about the command descriptions in this reference (see “Understanding Command Descriptions” on page 36)

Overview

Mobility System Software (MSS) operates a 3Com Mobility System wireless LAN (WLAN) consisting of 3Com Wireless Switch Manager (3WXM) software and 3Com Wireless LAN Switch or 3Com Wireless LAN Controller (WX switch) and 3Com Wireless LAN Managed Access Point (MAP) hardware. There is a command-line interface (CLI) on the WX switch that you can use to configure and manage the WX and its attached access points.

You configure the wireless LAN switches and access points primarily with **set**, **clear**, and **display** commands. Use **set** commands to change parameters. Use **clear** commands to reset parameters to their defaults. In many cases, you can overwrite a parameter with another **set** command. Use **display** commands to show the current configuration and monitor the status of network operations.

The wireless LAN switches support two connection modes:

- Administrative access mode, which enables the network administrator to connect *to* the WX switch and configure the network
- Network access mode, which enables network users to connect *through* the WX switch to access the network

CLI Conventions

Be aware of the following MSS CLI conventions for command entry:

- “Command Prompts” on page 28
- “Syntax Notation” on page 28
- “Text Entry Conventions and Allowed Characters” on page 29
- “User Globs, MAC Address Globs, and VLAN Globs” on page 30
- “Port Lists” on page 32
- “Virtual LAN Identification” on page 33

Command Prompts

By default, the MSS CLI provides the following prompt for restricted users. The *mmm* portion shows the wireless LAN switch model number (for example, *1200*).

```
WXmmm>
```

After you become enabled as an administrative user by typing **enable** and supplying a suitable password, MSS displays the following prompt:

```
WXmmm#
```

For information about changing the CLI prompt on a wireless LAN switch, see “set prompt” on page 59.

Syntax Notation

The MSS CLI uses standard syntax notation:

- Bold monospace font identifies the command and keywords you must type. For example:

```
set enablepass
```

- Italics indicate a placeholder for a value. For example, you replace *vlan-id* in the following command with a virtual LAN (VLAN) ID:

```
clear interface vlan-id ip
```

- Curly brackets (**{ }**) indicate a mandatory parameter, and square brackets (**[]**) indicate an optional parameter. For example, you must enter **dynamic** or **port** and a port list in the following command, but a VLAN ID is optional:

```
clear fdb {dynamic | port port-list} [vlan vlan-id]
```

- A vertical bar (|) separates mutually exclusive options within a list of possibilities. For example, you enter either **enable** or **disable**, not both, in the following command:

```
set port {enable | disable} port-list
```

Text Entry Conventions and Allowed Characters

Unless otherwise indicated, the MSS CLI accepts standard ASCII alphanumeric characters, except for tabs and spaces, and is case-insensitive.

The CLI has specific notation requirements for MAC addresses, IP addresses, and masks, and allows you to group usernames, MAC addresses, virtual LAN (VLAN) names, and ports in a single command.

3Com recommends that you do not use the same name with different capitalizations for VLANs or access control lists (ACLs). For example, do not configure two separate VLANs with the names *red* and *RED*.

The CLI does not support the use of special characters including the following in any named elements such as SSIDs and VLANs: ampersand (&), angle brackets (< >), number sign (#), question mark (?), or quotation marks ("").

In addition, the CLI does not support the use of international characters such as the accented *É* in *DÉCOR*.

MAC Address Notation

MSS displays MAC addresses in hexadecimal numbers with a colon (:) delimiter between bytes — for example, 00:01:02:1a:00:01. You can enter MAC addresses with either hyphen (-) or colon (:) delimiters, but colons are preferred.

For shortcuts:

- You can exclude leading zeros when typing a MAC address. MSS displays of MAC addresses include all leading zeros.
- In some specified commands, you can use the single-asterisk (*) wildcard character to represent from 1 byte to 5 bytes of a MAC address. (For more information, see “MAC Address Globs” on page 31.)

IP Address and Mask Notation

MSS displays IP addresses in dotted decimal notation — for example, 192.168.1.111. MSS makes use of both subnet masks and wildcard masks.

Subnet Masks

Unless otherwise noted, use classless interdomain routing (CIDR) format to express subnet masks — for example, 192.168.1.112/24. You indicate the subnet mask with a forward slash (*/*) and specify the number of bits in the mask.

Wildcard Masks

Security access control lists (ACLs) use source and destination IP addresses and wildcard masks to determine whether the wireless LAN switch filters or forwards IP packets. Matching packets are either permitted or denied network access. The ACL checks the bits in IP addresses that correspond to any 0s (zeros) in the mask, but does not check the bits that correspond to 1s (ones) in the mask. You specify the wildcard mask in dotted decimal notation.

For example, the address 10.0.0.0 and mask 0.255.255.255 match all IP addresses that begin with 10 in the first octet.

The ACL mask must be a contiguous set of zeroes starting from the first bit. For example, 0.255.255.255, 0.0.255.255, and 0.0.0.255 are valid ACL masks. However, 0.255.0.255 is not a valid ACL mask.

User Globs, MAC Address Globs, and VLAN Globs

Name “globbing” is a way of using a wildcard pattern to expand a single element into a list of elements that match the pattern. MSS accepts user globs, MAC address globs, and VLAN globs. The order in which globs appear in the configuration is important, because once a glob is matched, processing stops on the list of globs.

User Globs

A user glob is shorthand method for matching an authentication, authorization, and accounting (AAA) command to either a single user or a set of users.

A user glob can be up to 80 characters long and cannot contain spaces or tabs. The double-asterisk (******) wildcard characters with no delimiter characters match *all* usernames. The single-asterisk (*****) wildcard character matches any number of characters up to, but not including, a delimiter character in the glob. Valid user glob delimiter characters are the *at* (**@**) sign and the period (**.**).

Table 3 gives examples of user globs.

Table 3 User Globs

User Glob	User(s) Designated
jose@example.com	User <i>jose</i> at example.com
*@example.com	All users at example.com whose usernames do not contain periods — for example, jose@example.com and tamara@example.com, but <i>not</i> nin.wong@example.com, because nin.wong contains a period
*@marketing.example.com	All marketing users at example.com whose usernames do not contain periods
.@marketing.example.com	All marketing users at example.com whose usernames contain periods
*	All users with usernames that have no delimiters
EXAMPLE*	All users in the Windows Domain EXAMPLE with usernames that have no delimiters
EXAMPLE*.*	All users in the Windows Domain EXAMPLE whose usernames contain periods
**	All users

MAC Address Globs

A media access control (MAC) address glob is a similar method for matching some authentication, authorization, and accounting (AAA) and forwarding database (FDB) commands to one or more 6-byte MAC addresses. In a MAC address glob, you can use a single asterisk (*) as a wildcard to match *all* MAC addresses, or as follows to match from 1 byte to 5 bytes of the MAC address:

```
00:*
00:01:*
00:01:02:*
00:01:02:03:*
00:01:02:03:04:*
```

For example, the MAC address glob 02:06:8c* represents all MAC addresses starting with 02:06:8c. Specifying only the first 3 bytes of a MAC address allows you to apply commands to MAC addresses based on an organizationally unique identity (OUI).

VLAN Globs

A VLAN glob is a method for matching one of a set of local rules on an wireless LAN switch, known as the location policy, to one or more users. MSS compares the VLAN glob, which can optionally contain wildcard characters, against the VLAN-Name attribute returned by AAA, to determine whether to apply the rule.

To match all VLANs, use the double-asterisk (******) wildcard characters with no delimiters. To match any number of characters up to, but not including, a delimiter character in the glob, use the single-asterisk (*****) wildcard. Valid VLAN glob delimiter characters are the *at* (**@**) sign and the period (**.**).

For example, the VLAN glob *bdg4.** matches *bdg4.security* and *bdg4.hr* and all other VLAN names with *bdg4.* at the beginning.

Matching Order for Globs

In general, the order in which you enter AAA commands determines the order in which MSS matches the user, MAC address, or VLAN to a glob. To verify the order, view the output of the **display aaa** or **display config** command. MSS checks globs that appear higher in the list before items lower in the list and uses the first successful match.

Port Lists

The physical Ethernet ports on a WX switch can be set for connection to MAP access points, authenticated wired users, or the network backbone. You can include a single port or multiple ports in one MSS CLI command by using the appropriate list format.

The ports on a WX switch are numbered 1 through 4 (for the 3Com Wireless LAN Controller WX4400) and 1 through 8 (for the 3Com Wireless Lan Switch WX1200). No port 0 exists on the WX switch. You can include a single port or multiple ports in a command that includes **port port-list**. Use one of the following formats for **port-list**:

- A single port number. For example:

```
WX1200# set port enable 6
```
- A comma-separated list of port numbers, with no spaces. For example:

```
WX1200# display port poe 1,2,4
```


- A hyphen-separated range of port numbers, with no spaces. For example:

```
WX1200# reset port 1-3
```

- Any combination of single numbers, lists, and ranges. Hyphens take precedence over commas. For example:

```
WX1200# display port status 1-3,6
```

Virtual LAN Identification

The *names* of virtual LANs (VLANs), which are used in Mobility Domain™ communications, are set by you and can be changed. In contrast, VLAN ID *numbers*, which the wireless LAN uses locally, are determined when the VLAN is first configured and cannot be changed. Unless otherwise indicated, you can refer to a VLAN by either its VLAN name or its VLAN number. CLI **set** and **display** commands use a VLAN's name or number to uniquely identify the VLAN within the WX.

Command-Line Editing

MSS editing functions are similar to those of many other network operating systems.

Keyboard Shortcuts

The following table lists the keyboard shortcuts for entering and editing CLI commands.

Table 4 Keyboard Shortcuts

Keyboard Shortcut(s)	Function
Ctrl+A	Jumps to the first character of the command line.
Ctrl+B or Left Arrow key	Moves the cursor back one character.
Ctrl+C	Escapes and terminates prompts and tasks.
Ctrl+D	Deletes the character at the cursor.
Ctrl+E	Jumps to the end of the current command line.
Ctrl+F or Right Arrow key	Moves the cursor forward one character.
Ctrl+K	Deletes from the cursor to the end of the command line.
Ctrl+L or Ctrl+R	Repeats the current command line on a new line.
Ctrl+N or Down Arrow key	Enters the next command line in the history buffer.
Ctrl+P or Up Arrow key	Enters the previous command line in the history buffer.

Table 4 Keyboard Shortcuts (continued)

Keyboard Shortcut(s)	Function
Ctrl+U or Ctrl+X	Deletes characters from the cursor to the beginning of the command line.
Ctrl+W	Deletes the last word typed.
Esc B	Moves the cursor back one word.
Esc D	Deletes characters from the cursor forward to the end of the word.
Delete key or Backspace key	Erases mistake made during command entry. Reenter the command after using this key.

History Buffer

The history buffer stores the last 63 commands you entered during a terminal session. You can use the Up Arrow and Down Arrow keys to select a command that you want to repeat from the history buffer.

Tabs

The MSS CLI uses the Tab key for command completion. You can type the first few characters of a command and press the Tab key to show the command(s) that begin with those characters. For example:

```
WX1200# display i <Tab>
ifm          display interfaces maintained by the interface
manager
igmp         display igmp information
interface    display interfaces
ip           display ip information
```

Single-Asterisk (*) Wildcard Character

You can use the single-asterisk (*) wildcard character in globbing. (For details, see “User Globs, MAC Address Globs, and VLAN Globs” on page 30.)

Double-Asterisk () Wildcard Characters**

The double-asterisk (**) wildcard character matches all usernames. For details, see “User Globs” on page 30.

Using CLI Help

The CLI provides online help. To see the full range of commands available at your access level, type the **help** command. For example:

```
WX1200# help
Commands:
-----
clear          Clear, use 'clear help' for more information
commit        Commit the content of the ACL table
copy          Copy from filename (or url) to filename (or url)
crypto        Crypto, use 'crypto help' for more information
delete        Delete url
dir           Show list of files on flash device
disable       Disable privileged mode
display       Display, use 'display help' for more information
exit         Exit from the Admin session
help         Show this help screen
history       Show contents of history substitution buffer
load         Load, use 'load help' for more information
logout       Exit from the Admin session
monitor      Monitor, use 'monitor help' for more information
ping         Send echo packets to hosts
quit         Exit from the Admin session
reset        Reset, use 'reset help' for more information
rollback     Remove changes to the edited ACL table
save         Save the running configuration to persistent storage
set          Set, use 'set help' for more information
telnet       telnet IP address [server port]
traceroute   Print the route packets take to network host
```

For more information on help, see “help” on page 50.

To see a subset of the online help, type the command for which you want more information. For example, to show all the commands that begin with the letter *i*, type the following command:

```
WX1200# display i?
ifm          Show interfaces maintained by the interface manager
igmp         Show igmp information
interface    Show interfaces
ip           Show ip information
```

To see all the variations, type one of the commands followed by a question mark (?). For example:

```
WX1200# display ip ?
alias          display ip aliases
dns            display DNS status
https         display ip https
route         display ip route table
telnet        display ip telnet
```

To determine the port on which Telnet is running, type the following command:

```
WX1200# display ip telnet
Server Status          Port
-----
Enabled                23
```

Understanding Command Descriptions

Each command description in the *3Com Mobility System Software Command Reference* contains the following elements:

- A command name, which shows the keywords but not the variables. For example, the following command name appears at the top of a command description and in the index:


```
set ap name
```
- A brief description of the command's functions.
- The full command syntax.
- Any command defaults.
- The command access, which is either *enabled* or *all*. *All* indicates that anyone can access this command. *Enabled* indicates that you must enter the enable password before entering the command.
- The command history, which identifies the MSS version in which the command was introduced and the version numbers of any subsequent updates.
- Special tips for command usage. These are omitted if the command requires no special usage.
- One or more examples of the command in context, with the appropriate system prompt and response.
- One or more related commands.

2

ACCESS COMMANDS

This chapter describes access commands used to control access to the Mobility Software System (MSS) command-line interface (CLI).

Commands by Usage

This chapter presents access services commands alphabetically. Use Table 5 to located commands in this chapter based on their use.

Table 5 Access Commands by Usage

Type	Command
Access Privileges	enable on page 38
	set enablepass on page 39
	disable on page 37
	quit on page 38

disable

Changes the CLI session from enabled mode to restricted access.

Syntax — `disable`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command restricts access to the CLI for the current session:

```
WX1200# disable
WX1200>
```

See Also

- **enable** on page 38

enable

Places the CLI session in enabled mode, which provides access to all commands required for configuring and monitoring the system.

Syntax — `enable`

Access — All.

History — Introduced in MSS Version 3.0.

Usage — MSS displays a password prompt to challenge you with the enable password. To enable a session, your or another administrator must have configured the enable password to this WX switch with the **set enablepass** command.

Examples — The following command plus the enable password provides enabled access to the CLI for the current sessions:

```
WX1200> enable
Enter password: password
WX1200#
```

See Also

- **set enablepass** on page 39
- **set confirm** on page 57

quit

Exit from the CLI session.

Syntax — `quit`

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — To end the administrator's session, type the following command:

```
WX1200> quit
```

set enablepass

Sets the password that provides enabled access (for configuration and monitoring) to the WX switch.

Syntax — `set enablepass`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — After typing the **set enablepass** command, press Enter. If you are entering the first enable password on this WX switch, press Enter at the **Enter old password** prompt. Otherwise, type the old password. Then type a password of up to 32 alphanumeric characters with no spaces, and reenter it at the **Retype new password** prompt.



CAUTION: *Be sure to use a password that you will remember. If you lose the enable password, the only way to restore it causes the system to return to its default settings and wipes out the configuration.*

Examples — The following example illustrates the prompts that the system displays when the enable password is changed. The passwords you enter are not displayed.

```
WX1200# set enablepass
Enter old password: old-password
Enter new password: new-password
Retype new password: new-password
Password changed
```

See Also

- **disable** on page 37
- **enable** on page 38

3

SYSTEM SERVICE COMMANDS

Use system services commands to configure and monitor system information for a WX switch.

Commands by Usage

This chapter presents system service commands alphabetically. Use Table 6 to locate commands in this chapter based on their use.

Table 6 System Services Commands by Usage

Type	Command
Configuration	quickstart on page 52
Auto-Config	set auto-config on page 52
Display	clear banner motd on page 42
	quickstart on page 52
	display banner motd on page 45
	set banner acknowledge on page 54
	set confirm on page 57
	set length on page 57
System Identification	set prompt on page 59
	set system name on page 68
	set system location on page 67
	set system contact on page 60
	set system countrycode on page 61
	set system idle-timeout on page 65
	set system idle-timeout on page 65
	display load on page 47
display system on page 47	

Table 6 System Services Commands by Usage (continued)

Type	Command
	clear system on page 44
	clear prompt on page 43
Help	help on page 50
History	history on page 51
	clear history on page 43
License	display license on page 46
	set license on page 58
Technical Support	display base-information on page 45

clear banner motd

Deletes the message-of-the-day (MOTD) banner that is displayed before the login prompt for each CLI session on the wireless LAN switch.

Syntax — `clear banner motd`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To clear a banner, type the following command:

```
WX4400# clear banner motd
success: change accepted
```



As an alternative to clearing the banner, you can overwrite the existing banner with an empty banner by typing the following command:

set banner motd ^^

See Also

- **display banner motd** on page 45
- **quickstart** on page 52

clear history

Deletes the command history buffer for the current CLI session.

Syntax — `clear history`

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — To clear the history buffer, type the following command:

```
WX4400# clear history
success: command buffer was flushed.
```

See Also

- **history** on page 51

clear prompt

Resets the system prompt to its previously configured value. If the prompt was not configured previously, this command resets the prompt to its default.

Syntax — `clear prompt`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To reset the prompt, type the following command:

```
wildebeest# clear prompt
success: change accepted.
WX4400#
```

See Also

- **set prompt** on page 59. (For information about default prompts, see “Command Prompts” on page 28.)

clear system

Clears the system configuration of the specified information.



CAUTION: *If you change the IP address, any currently configured Mobility Domain operations cease. You must reset the Mobility Domain.*

Syntax — `clear system [contact | countrycode | idle-timeout | ip-address | location | name]`

- **contact** — Resets the name of contact person for the WX switch to null.
- **countrycode** — Resets the country code for the WX switch to null.
- **idle-timeout** — Resets the number of seconds a CLI management session can remain idle to the default value (3600 seconds).
- **ip-address** — Resets the IP address of the WX switch to null.
- **location** — Resets the location of the WX switch to null.
- **name** — Resets the name of the WX switch to the default system name, which is the model number.

Defaults — None.

Access — Enabled.

History — —Introduced in MSS Version 3.0. Option `idle-timeout` added in MSS Version 4.1.

Examples — To clear the location of the WX switch, type the following command:

```
WX4400# clear system location
success: change accepted.
```

See Also

- **display config** on page 675
- **display system** on page 47
- **set system contact** on page 60
- **set system countrycode** on page 61
- **set system idle-timeout** on page 65
- **set system idle-timeout** on page 65
- **set system location** on page 67

display banner motd

Shows the banner that was configured with the **set banner motd** command.

Syntax — `display banner motd`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To show the banner with the message of the day, type the following command:

```
WX4400# display banner motd
hello world
```

See Also

- **clear banner motd** on page 42
- **quickstart** on page 52

display base-information

Provides an in-depth snapshot of the status of the wireless LAN switch, which includes details about the boot image, the version, ports, and other configuration values. This command also displays the last 100 log messages.

Syntax — `display base-information`
[**file** [*subdirname/*] *filename*]

- [*subdirname/*] *filename* — Optional subdirectory name, and a string up to 32 alphanumeric characters. The command's output is saved into a file with the specified name in nonvolatile storage.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Enter this command before calling for Technical Support. See "Obtaining Support for Your 3Com Products" on page 739 for more information.

See Also

- **display boot** on page 674
- **display config** on page 675
- **display license** on page 46
- **display system** on page 47
- **display version** on page 677

display license

Displays information about the license currently installed on the WX switch.

Syntax — `display license`

Defaults — None.

Access — All.

Examples — To view the WX switch license, type the following command:

```
WX4400# display license
Serial Number      : M8XE4IBB8DB10

License Number    : 245
License Key       : WXL-076E-93E9-62DA-54D8
Activation key    : WXA-3E04-4CC2-430D-B508
Feature           : 24 additional ports
Expires           : Never
```

The additional ports refers to the number of additional MAPs the switch can boot and actively manage.

See Also

- **set license** on page 58

display load

Displays CPU usage on a WX switch.

Syntax — `display load`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.1.

Examples — To display the CPU load recorded from the time the WX switch was booted, as well as from the previous time the **display load** command was run, type the following command:

```
WX4400# display load
System Load: overall: 2% delta: 5%
```

The overall field shows the CPU load as a percentage from the time the WX switch was booted. The delta field shows CPU load as a percentage from the last time the **display load** command was entered.

See Also

- **display system** on page 47

display system

Shows system information.

Syntax — `display system`

Defaults — None.

Access — Enabled.

Examples — To show system information, type the following command:

```
WX4400# display system
=====
Product Name:      WX4400
System Name:       WX-bldg3
System Countrycode: US
System Location:   first-floor-bldg3
System Contact:    tamara@example.com
System IP:         192.168.12.7
System idle timeout: 3600
System MAC:        00:0B:0E:00:04:30
=====
Boot Time:         2003-11-07 15:45:49
Uptime:           13 days 04:29:10
=====
Fan status: fan1 OK fan2 OK fan3 OK
Temperature: temp1 ok temp2 ok temp3 ok
PSU Status: Lower Power Supply DC ok AC ok Upper Power Supply missing
Memory:           97.04/744.03 (13%)
Total Power Over Ethernet : 29.000
=====
```

Table 7 describes the fields of **display system output**.

Table 7 display system output

Field	Description
Product Name	Switch model number.
System Name	System name (factory default, or optionally configured with set system name).
System Countrycode	Country-specific 802.11 code required for MAP operation (configured with set system countrycode).
System Location	Record of the WX switch's physical location (optionally configured with set system location).
System Contact	Contact information about the system administrator or another person to contact about the system (optionally configured with set system contact).
System IP	Common interface, source, and default IP address for the device, in dotted decimal notation (configured with set system ip-address).

Table 7 display system output (continued)

Field	Description
System idle timeout	Number of seconds MSS allows a CLI management session (console, Telnet, or SSH) to remain idle before terminating the session. (The system idle timeout can be configured using the set system idle-timeout command.)
System MAC	WX switch's media access control (MAC) machine address set at the factory, in 6-byte hexadecimal format.
License	License level installed on the WX switch (if applicable).
Boot Time	Date and time of the last system reboot.
Uptime	Number of days, hours, minutes, and seconds that the WX has been operating since its last restart.
Fan status	<p>Operating status of the WX switch's three cooling fans:</p> <ul style="list-style-type: none"> ▪ OK — Fan is operating. ▪ Failed — Fan is not operating. MSS sends an alert to the system log every 5 minutes until this condition is corrected. <p>Fan 1 is located nearest the front of the chassis, and fan 3 is located nearest the back.</p>
Temperature	<p>Status of temperature sensors at three locations in the WX switch:</p> <ul style="list-style-type: none"> ▪ ok — Temperature is within the acceptable range of 0° C to 50° C (32° F to 122° F). ▪ Alarm — Temperature is above or below the acceptable range. MSS sends an alert to the system log every 5 minutes until this condition is corrected.
PSU Status	<p>Status of the lower and upper power supply units:</p> <ul style="list-style-type: none"> ▪ missing — Power supply is not installed or is inoperable. ▪ DC ok — Power supply is producing DC power. ▪ DC output failure — Power supply is not producing DC power. MSS sends an alert to the system log every 5 minutes until this condition is corrected. ▪ AC ok — Power supply is receiving AC power. ▪ AC not present — Power supply is not receiving AC power.

Table 7 display system output (continued)

Field	Description
Memory	Current size (in megabytes) of nonvolatile memory (NVRAM) and synchronous dynamic RAM (SDRAM), plus the percentage of total memory space in use, in the following format: <i>NVRAM size /SDRAM size (percent of total)</i>
Total Power Over Ethernet	Total power that the device is currently supplying to its directly connected MAP access points, in watts.

See Also

- **clear system** on page 44
- **set system contact** on page 60
- **set system countrycode** on page 61
- **set system idle-timeout** on page 65
- **set system location** on page 67
- **set system name** on page 68

help

Displays a list of commands that can be used to configure and monitor the WX switch.

Syntax — `help`

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — Use this command to see a list of available commands. If you have restricted access, you see fewer commands than if you have enabled access. To show a list of CLI commands available at the enabled access level, type the following command at the enabled access level:

```
WX4400# help
```

```
Commands:
```

```
-----
clear          Clear, use 'clear help' for more information
commit        Commit the content of the ACL table
copy          Copy from filename (or url) to filename (or url)
```

crypto	Crypto, use 'crypto help' for more information
delete	Delete url
dir	Show list of files on flash device
disable	Disable privileged mode
display	Display, use 'display help' for more information
disp tech support	Display technical support information
exit	Exit from the Admin session
help	Show this help screen
history	Show contents of history substitution buffer
hit-sample-rate	Set NP hit-counter sample rate
load	Load, use 'load help' for more information
logout	Exit from the Admin session
monitor	Monitor, use 'monitor help' for more information
ping	Send echo packets to hosts
quit	Exit from the Admin session
reset	Reset, use 'reset help' for more information
rollback	Remove changes to the edited ACL table
save	Save the running configuration to persistent storage
set	Set, use 'set help' for more information
telnet	telnet IP address [server port]
traceroute	Print the route packets take to network host

See Also

- **Using CLI Help** on page 35

history

Displays the command history buffer for the current CLI session.

Syntax — `history`

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — To show the history of your session, type the following command:

```
WX4400> history
Display History (most recent first)
-----
[00] display config
[01] display version
[02] enable
```

See Also

- **clear history** on page 43

quickstart

Runs a script that interactively helps you configure a new switch.

(For more information, see the “CLI quickstart Command” section of the “WX Setup Methods” chapter in the [Wireless LAN Switch and Controller Configuration Guide](#).)



CAUTION: *The quickstart command is for configuration of a new switch only. After prompting you for verification, the command erases the switch’s configuration before continuing. If you run this command on a switch that already has a configuration, the configuration will be erased. In addition, error messages such as “Critical AP Notice” for directly connected MAPs can appear.*

set auto-config

Enables a WX switch to contact a 3WXM server for its configuration.

Syntax — `set auto-config {enable | disable}`

- **enable** — Enables the switch to contact a 3WXM server to request a configuration.
- **disable** — Disables the auto-config option.

Defaults — The auto-config option is automatically enabled on an unconfigured WXR100 when the factory reset switch is pressed during power on. However, auto-config is disabled by default on other models.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — A network administrator at the corporate office can preconfigure the switch in a 3WXM network plan. The switch configuration must have a name for the switch, the model must be WXR100, and the serial number must match the switch’s serial number. The configuration should also include all other settings required for the deployment, including MAP configuration, SSIDs, AAA settings, and so on.

When the 3WXM server in the corporate network receives the configuration request, the server looks in the currently open network plan for a switch configuration with the same model and serial number as the one in the configuration request.

- If the network plan contains a configuration with a matching model and serial number, 3WXM sends the configuration to the switch and restarts the switch. The switch boots using the configuration it received from 3WXM.
- If the network plan does not have a configuration with a matching model and serial number, a verification warning appears in 3WXM. The warning lists the switch's serial number and IP address. The network administrator can upload the switch into the network plan, configure switch parameters, and deploy the configuration to the switch.

To use the auto-config option with a new (unconfigured) WXR100, insert a paperclip or similar object into the WXR100's factory reset hole to press the switch. The factory reset switch must be held for about 3 seconds while the factory reset LED (the right LED above port 1) is lit. Normally, this LED remains solidly lit for 3 seconds after power on. However, when the factory reset switch is pressed, the LED flashes for 3 seconds instead.

If you want another WX switch model to be able to access a 3WXM server for a configuration, you also must preconfigure the WX with the following information:

- IP address
- Gateway address
- Domain name and DNS server address

You can enable the switch to use the MSS DHCP client to obtain this information from a DHCP server in the local network where the switch will be deployed. Alternatively, you can statically configure the information.

The IP address and DNS information are configured independently. You can configure the combination of settings that work with the network resources available at the deployment site. The following examples show some of the combinations you can configure.

Examples — The following commands stage a WX switch to use the auto-config option. The network where the switch is installed has a DHCP server, so the switch is configured to use the MSS DHCP client to obtain an IP address, default gateway address, DNS domain name, and DNS server IP addresses:

1 Configure a VLAN:

```
WX-1200# set vlan 1 port 7
success: change accepted.
```

2 Enable the DHCP client on VLAN 1:

```
WX-1200# set interface 1 ip dhcp-client enable
success: change accepted.
```

3 Enable the auto-config option:

```
WX-1200# set auto-config enable
success: change accepted.
```

4 Save the configuration changes:

```
WX-1200# save config
success: configuration saved.
```

See Also

- **crypto generate key** on page 565
- **crypto generate self-signed** on page 568
- **save config** on page 685
- **set interface dhcp-client** on page 171
- **set vlan port** on page 125

**set banner
acknowledge**

Configures a prompt that is displayed following the MOTD banner. The user must acknowledge the prompt in order to gain access to the system.

Syntax — `set banner acknowledge mode {enable | disable}`

Syntax — `set banner acknowledge message "message"`

- **enable** — Enables the prompt to acknowledge the MOTD banner.
- **disable** — Disables the prompt to acknowledge the MOTD banner.
- **"** — Delimiting character that begins and ends the prompt message; for example, double quotes (").

- *message* — Up to 32 alphanumeric characters, but *not* the delimiting character.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage Enable the MOTD prompt, then optionally specify a prompt message.

When a user logs into the WX switch using the CLI, the configured MOTD banner is displayed, followed by the MOTD prompt message (if one is specified). In response, the user has the option of entering **y** to proceed or any other key to terminate the connection.

Examples — To enable the prompt for the MOTD banner, type the following command:

```
WX# set banner acknowledge enable
success: change accepted.
```

To set *Do you agree?* as the text to be displayed following the MOTD banner, type the following command:

```
WX# set banner acknowledge message "Do you agree?"
success: change accepted.
```

After these commands are entered, when the user logs on, the MOTD banner is displayed, followed by the text *Do you agree?* If the user enters *y*, then the login proceeds; if not, then the user is disconnected.

See Also

- **set banner motd** on page 56
- **clear banner motd** on page 42
- **display banner motd** on page 45

set banner motd

Configures the banner string that is displayed before the beginning of each login prompt for each CLI session on the WX switch.

Syntax — `set banner motd "text"`

- `"` — Delimiting character that begins and ends the message; for example, double quotes (`"`).
- `text` — Up to 2000 alphanumeric characters, including tabs and carriage returns, but *not* the delimiting character (`^`). The maximum number of characters is approximately 24 lines by 80 characters.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Type a delimiting character, then the message, then another delimiting character.

Examples — To create a banner that says *Meeting @ 4:00 p.m. in Conference Room #3*, type the following command:

```
WX# set banner motd "Meeting @ 4:00 p.m. in Conference Room #3"
success: motd changed.
```

See Also

- **set banner acknowledge** on page 54
- **clear banner motd** on page 42
- **display banner motd** on page 45

set confirm

Enables or disables the display of confirmation messages for commands that might have a large impact on the network.

Syntax — `set confirm {on | off}`

- **on** — Enables confirmation messages.
- **off** — Disables confirmation messages.

Defaults — Configuration messages are enabled.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command remains in effect for the duration of the session, until you enter a **quit** command, or until you enter another **set confirm** command.

MSS displays a message requiring confirmation when you enter certain commands that can have a potentially large impact on the network. For example:

```
WX4400# clear vlan red
This may disrupt user connectivity.
Do you wish to continue? (y/n) [n]
```

Examples — To turn off these confirmation messages, type the following command:

```
WX4400# set confirm off
success: Confirm state is off
```

set length

Defines the number of lines of CLI output to display between paging prompts. MSS displays the set number of lines and waits for you to press any key to display another set, or type **q** to quit the display.

Syntax — `set length number-of-lines`

- *number-of-lines* — Number of lines of text to display between paging prompts. You can specify from 0 to 512. The 0 value disables the paging prompt action entirely.

Defaults — MSS displays 24 lines by default.

Access — All.

History — Introduced in MSS Version 3.0.

Usage — Use this command if the output of a CLI command is greater than the number of lines allowed by default for a terminal type.

Examples — To set the number of lines displayed to 100, type the following command:

```
WX4400# set length 100
success: screen length for this session set to 100
```

set license

Installs an upgrade license, for managing more MAPs.

Syntax — `set license license-key activation-key`

- *license-key* — License key, starting with WXL. You can enter the key with or without the hyphens.
- *activation-key* — Activation key, starting with WXA. You can enter the key with or without the hyphens.

Defaults — The WX4400 can boot and manage 24 MAPs by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The license key is shipped with the switch. To obtain the activation key, access the 3Com web site. Each license and activation key pair allows the switch to actively manage an additional 24 MAPs. You can install up to three upgrade license and activation key pairs, to actively manage up to 96 MAPs.

Examples — To install an upgrade license and activation key, type the following command:

```
WX4400# set license WXL-076E-93E9-62DA-54D8
WXA-3E04-4CC2-430D-B508
Serial Number      : M8XE4IBB8DB10

License Number    : 245
License Key       : WXL-076E-93E9-62DA-54D8
Activation key    : WXA-3E04-4CC2-430D-B508
Feature          : 24 additional ports
Expires          : Never
```

```
48 ports are enabled
success: license was installed
```

The additional ports refers to the number of additional MAPs the switch can boot and actively manage.

See Also

- **display license** on page 46

set prompt

Changes the CLI prompt for the WX switch to a string you specify.

Syntax — `set prompt string`

- *string* — Alphanumeric string up to 32 characters long. To include spaces in the prompt, you must enclose the string in double quotation marks ("").

Defaults — The factory default for the WX switch name is the model number (*WX1200* for the 3Com Wireless LAN Switch *WX1200*, *WX4400* for the 3Com Wireless LAN Controller *WX4400*).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — When you first log in for the initial configuration of the WX switch, the CLI provides a *WX1200>* or *WX4400>* prompt, depending on your model. After you become enabled by typing **enable** and giving a suitable password, the *WX1200#* or *WX4400#* prompt is displayed.

If you use the **set system name** command to change the default system name, MSS uses that name in the prompt, unless you also change the prompt with **set prompt**.

Examples — The following example sets the prompt from *WX4400* to *happy_days*:

```
WX4400# set prompt happy_days
success: change accepted.
happy_days#
```

See Also

- **clear prompt** on page 43

- **display config** on page 675
- **set system name** on page 68

set system contact

Stores a contact name for the WX switch.

Syntax — `set system contact string`

- *string* — Alphanumeric string up to 256 characters long, with no blank spaces.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

To view the system contact string, type the **display system** command.

Examples — The following command sets the system contact information to *tamara@example.com*:

```
WX1200# set system contact tamara@example.com
success: change accepted.
```

See Also

- **clear system** on page 44
- **display system** on page 47
- **set system location** on page 67
- **set system name** on page 68

**set system
countrycode**

Defines the country-specific IEEE 802.11 regulations to enforce on the WX switch.

Syntax — `set system countrycode code`

- `code` — Two-letter code for the country of operation for the WX switch. You can specify one of the codes listed in Table 8.

Table 8 Country Codes

Country	Code
Algeria	DZ
Argentina	AR
Australia	AU
Austria	AT
Bahrain	BH
Belgium	BE
Belize	BZ
Bolivia	BO
Boznia and Herzegovina	BA
Brazil	BR
Bulgaria	BG
Canada	CA
Chile	CL
China	CN
Colombia	CO
Costa Rica	CR
Cote d'Ivoire	CI
Croatia	HR
Cyprus	CY
Czech Republic	CZ
Denmark	DK
Dominican Republic	DO
Ecuador	EC
El Salvador	SV

(continued)

Table 8 Country Codes (continued)

Country	Code
Egypt	EG
Estonia	EE
Finland	FI
France	FR
Germany	DE
Greece	GR
Guatemala	GT
Honduras	HN
Hong Kong	HK
Hungary	HU
Iceland	IS
India	IN
Indonesia	ID
Ireland	IE
Israel	IL
Italy	IT
Jamaica	JM
Japan	JP
Jordan	JO
Kazakhstan	KZ
Kenya	KE
Kuwait	KW
Latvia	LV
Lebanon	LB
Liechtenstein	LI
Lithuania	LT
Luxembourg	LU
Macedonia, former Yugoslav Republic of	MK
Malaysia	MY
Malta	MT
Mauritius	MU

(continued)

Table 8 Country Codes (continued)

Country	Code
Mexico	MX
Morocco	MA
Namibia	NA
Netherlands	NL
New Zealand	NZ
Nigeria	NG
Norway	NO
Oman	OM
Pakistan	PK
Panama	PA
Paraguay	PY
Peru	PE
Philippines	PH
Poland	PL
Portugal	PT
Puerto Rico	PR
Qatar	QA
Romania	RO
Russia	RU
Saudi Arabia	SA
Serbia	CS
Singapore	SG
Slovakia	SK
Slovenia	SI
South Africa	ZA
South Korea	KR
Spain	ES
Sri Lanka	LK
Sweden	SE
Switzerland	CH
Taiwan	TW
Thailand	TH

(continued)

Table 8 Country Codes (continued)

Country	Code
Trinidad and Tobago	TT
Tunisia	TN
Turkey	TR
Ukraine	UA
United Arab Emirates	AE
United Kingdom	GB
United States	US
Uruguay	UY
Venezuela	VE
Vietnam	VN

Defaults — The factory default country code is None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must set the system county code to a valid value before using any **set ap** commands to configure a MAP.

Examples — To set the country code to Canada, type the following command:

```
WX1200# set system country code CA
success: change accepted.
```

See Also

- **display config** on page 675

**set system
idle-timeout**

Specifies the maximum number of seconds a CLI management session with the switch can remain idle before MSS terminates the session.

Syntax — `set system idle-timeout seconds`

- *seconds* — Number of seconds a CLI management session can remain idle before MSS terminates the session. You can specify from 0 to 86400 seconds (one day). If you specify 0, the idle timeout is disabled.

The timeout interval is in 30-second increments. For example, the interval can be 0, or 30 seconds, or 60 seconds, or 90 seconds, and so on. If you enter an interval that is not divisible by 30, the CLI rounds up to the next 30-second increment. For example, if you enter 31, the CLI rounds up to 60.

Defaults — 3600 seconds (one hour).

Access — Enabled.

History — Introduced in MSS Version 4.1.

Usage — This command applies to all types of CLI management sessions: console, Telnet, and SSH. The timeout change applies to existing sessions only, not to new sessions.

Examples — The following command sets the idle timeout to 1800 seconds (one half hour):

```
WX1200# set system idle-timeout 1800
success: change accepted.
```

See Also

- **clear system** on page 44
- **display system** on page 47

**set system
ip-address**

Sets the system IP address so that it can be used by various services in the WX switch.



CAUTION: *Any currently configured Mobility Domain operations cease if you change the IP address. If you change the address, you must reset the Mobility Domain.*

Syntax — `set system ip-address ip-addr`

- `ip-addr` — IP address, in dotted decimal notation.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command sets the IP address of the WX switch to 192.168.253.1:

```
WX4400# set system ip-address 192.168.253.1  
success: change accepted.
```

See Also

- **clear system** on page 44
- **set interface** on page 170
- **display system** on page 47

set system location Stores location information for the WX switch.

Syntax — `set system location string`

- *string* — Alphanumeric string up to 256 characters long, with no blank spaces.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You cannot include spaces in the system location string.

To view the system location string, type the **display system** command.

Examples — To store the location of the WX switch in the WX's configuration, type the following command:

```
WX4400# set system location first-floor-bldg3
success: change accepted.
```

See Also

- **clear system** on page 44
- **display system** on page 47
- **set system contact** on page 60
- **set system name** on page 68

set system name

Changes the name of the WX switch from the default system name and also provides content for the CLI prompt, if you do not specify a prompt.

Syntax — `set system name string`

- *string* — Alphanumeric string up to 256 characters long, with no blank spaces. Use a unique name for each WX switch.

Defaults — By default, the system name and command prompt have the same value. The factory default for both is the model number (*WX1200* for the 3Com Wireless LAN Switch WX1200, *WX4400* for the 3Com Wireless LAN Controller WX4400).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Entering **set system name** with no string resets the system name to the factory default.

To view the system name string, type the **display system** command.

Examples — The following example sets the system name to a name that identifies the WX switch:

```
WX4400# set system name WX-bldg3
success: change accepted.
WX-bldg3#
```

See Also

- **clear system** on page 44
- **display system** on page 47
- **set prompt** on page 59
- **set system contact** on page 60
- **set system location** on page 67

4

PORT COMMANDS

Use port commands to configure and manage individual ports and load-sharing port groups.

Commands by Usage

This chapter presents port commands alphabetically. Use Table 9 to locate commands in this chapter based on their use.

Table 9 Port Commands by Usage

Type	Command
Port Type	set port type ap on page 97
	set ap on page 87
	set port type wired-auth on page 100
	clear port type on page 74
	clear ap on page 70
Name	set port name on page 93
	clear port name on page 72
State	set port on page 89
	reset port on page 87
	display port status on page 79
Gigabit Interface Type	display port media-type on page 81
	set port media-type on page 91
	clear port media-type on page 72
Speed	set port speed on page 95
Autonegotiation	set port negotiation on page 93
PoE	set port poe on page 94
	display port poe on page 78
SNMP	set port trap on page 96

Table 9 Port Commands by Usage (continued)

Type	Command
Port Groups	set port-group on page 90
	display port-group on page 76
	clear port-group on page 71
Port Mirroring	display port mirror on page 77
	clear port mirror on page 73
	set port mirror on page 92
Statistics	display port counters on page 75
	monitor port counters on page 82
	clear port counters on page 71

clear ap

Removes a Distributed MAP.

**CAUTION:** When you clear a Distributed MAP, MSS ends user sessions that are using the MAP.**Syntax** — `clear ap {ap-number | all}`

- *ap-number* — Number of the Distributed MAP(s) to remove.
- **all** — Clear all distributed MAPs.

Defaults — None.**Access** — Enabled.**History** — Introduced in MSS Version 3.0. Version 6.0 renamed **dap** to **ap**.**Examples** — The following command clears Distributed MAP 1:

```
WX4400# clear ap 1
This will clear specified AP devices.
Would you like to continue? (y/n) [n]y
```

See Also

- **set ap** on page 87
- **set port type ap** on page 97

clear port counters Clears port statistics counters and resets them to 0.

Syntax — `clear port counters`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command clears all port statistics counters and resets them to 0:

```
WX4400# clear port counters
success: cleared port counters
```

See Also

- **display port counters** on page 75
- **monitor port counters** on page 82

clear port-group Removes a port group.

Syntax — `clear port-group name name`

- **name name** — Name of the port group.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command clears port group server1:

```
WX4400# clear port-group name server1
success: change accepted.
```

See Also

- **set port-group** on page 90
- **display port-group** on page 76

**clear port
media-type**

Disables the copper interface and reenables the fiber interface on an WX4400 gigabit Ethernet port.

Syntax — `clear port media-type port-list`

- *port-list*—List of physical ports. MSS disables the copper interface and reenables the fiber interface on all the specified ports.

Defaults — The GBIC (fiber) interface is enabled, and the copper interface is disabled, by default.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — This command applies only to the WX4400. This command does not affect a link that is already active on the port.

Examples — The following command disables the copper interface and reenables the fiber interface on port 2:

```
WX4400# clear port media-type 2
```

See Also

- **set port media-type** on page 91
- **display port media-type** on page 81

clear port name

Removes the name assigned to a port.

Syntax — `clear port port-list name`

- *port-list* — List of physical ports. MSS removes the names from all the specified ports.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command clears the names of ports 1 through 3:

```
WX4400# clear port 1-3 name
```

See Also

- **display port status** on page 79
- **set port name** on page 93

clear port mirror

Removes a port mirroring configuration.

Syntax — `clear port mirror`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Examples — The following command clears the port mirroring configuration from the switch:

```
WX4400# clear port mirror
```

See Also

- **display port mirror** on page 77
- **set port mirror** on page 92

clear port preference

Resets a gigabit Ethernet port on a WX4400 to use the GBIC (fiber) interface for the active link.

Syntax — `clear port preference port-list`

- *port-list* — List of physical ports. MSS clears the preference on all the specified ports.

Defaults — When both the copper and fiber interfaces of a gigabit Ethernet port are connected, the GBIC (fiber) interface is the active link. The RJ-45 (copper) link is unused.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command applies only to the WX4400. This command does not affect a link that is already active on the port.

Examples — The following command clears the preference set on port 2 on a WX4400 switch:

```
WX4400# clear port preference 2
```

See Also

- **display port status** on page 79

clear port type

Removes all configuration settings from a port and resets the port as a network port.



CAUTION: *When you clear a port, MSS ends user sessions that are using the port.*

Syntax — `clear port type port-list`

- *port-list* — List of physical ports. MSS resets and removes the configuration from all the specified ports.

Defaults — The cleared port becomes a network port but is not placed in any VLANs.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Use this command to change a port back to a network port. All configuration settings specific to the port type are removed. For example, if you clear a MAP access point port, all MAP-specific settings are removed. Table 10 lists the default network port settings that MSS applies when you clear a port's type.

Table 10 Network port defaults

Port Parameter	Setting
VLAN membership	None. Note: Although the command changes a port to a network port, the command does not place the port in any VLAN. To use the port in a VLAN, you must add the port to the VLAN.
Spanning Tree Protocol (STP)	Based on the VLAN(s) you add the port to.
802.1X	No authorization.
Port groups	None.
Internet Group Management Protocol (IGMP) snooping	Enabled as port is added to VLANs.
Access point and radio parameters	Not applicable
Maximum user sessions	Not applicable

Examples — The following command clears port 5:

```
WX1200# clear port type 5
This may disrupt currently authenticated users.
Are you sure? (y/n) [n]y
success: change accepted.
```

See Also

- **set port type ap** on page 97
- **set port type wired-auth** on page 100

display port counters

Displays port statistics.

Syntax — display port counters

```
[octets | packets | receive-errors | transmit-errors |
collisions | receive-etherstats |
transmit-etherstats] [port port-list]
```

- **octets** — Shows octet statistics.
- **packets** — Shows packet statistics.
- **receive-errors** — Shows errors in received packets.
- **transmit-errors** — Shows errors in transmitted packets.
- **collisions** — Shows collision statistics.

- **receive-etherstats** — Shows Ethernet statistics for received packets.
- **transmit-etherstats** — Shows Ethernet statistics for transmitted packets.
- **port *port-list*** — List of physical ports. If you do not specify a port list, MSS shows statistics for all ports.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Usage — You can specify one statistic type with the command.

Examples — The following command shows octet statistics for port 3:

```
WX1200> display port counters octets port 3
Port   Status                Rx Octets                Tx Octets
=====
    3   Up                    27965420                 34886544
```

This command's output has the same fields as the **monitor port counters** command. For descriptions of the fields, see Table 16 on page 84.

See Also

- **clear port counters** on page 71
- **monitor port counters** on page 82

display port-group

Shows port group information.

Syntax — **display port-group** [**name** *group-name*]

- **name** *group-name* — Shows information for the specified port group.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0. In Version 4.2 the option **all** was removed for simplicity. You can display information for all groups by entering the command without specifying a group name.

Examples — The following command displays the configuration of port group server2:

```
WX1200# display port-group name server2
Port group: server2 is up
    Ports: 5, 7
```

Table 11 describes the fields in the display port-group output.

Table 11 Output for display port-group

Field	Description
Port group	Name and state (enabled or disabled) of the port group.
Ports	Ports contained in the port group.

See Also

- **clear port-group** on page 71
- **set port-group** on page 90

display port mirror Displays the port mirroring configuration.

Syntax — `display port mirror`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Examples — The following command displays the port mirroring configuration on the switch:

```
WX4400# display port mirror
Port 1 is mirrored to port 2
```

If port mirroring is not configured, the message in the following example is displayed instead:

```
WX4400# display port mirror
No ports are mirrored
```

See Also

- **display port mirror** on page 77
- **set port mirror** on page 92

display port poe

Displays status information for ports on which Power over Ethernet (PoE) is enabled.

Syntax — `display port poe [port-list]`

- *port-list* — List of physical ports. If you do not specify a port list, PoE information is displayed for all ports.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays PoE information for all ports on a WX1200 switch:

```
WX1200# display port poe
      Link      Port      PoE      PoE
Port  Name      Status  Type     config   Draw
-----
  1   1              up       -        disabled off
  2   2              down     -        disabled off
  3   3              down     -        disabled off
  4   4              down     MAP      enabled  1.44
  5   5              down     -        disabled off
  6   6              down     -        disabled off
```

Table 12 describes the fields in this display.

Table 12 Output for display port poe

Field	Description
Port	Port number.
Name	Port name. If the port does not have a name, the port number is listed.

Table 12 Output for display port poe (continued)

Field	Description
Link status	Link status of the port: <ul style="list-style-type: none"> ▪ up—The port is connected. ▪ down—The port is not connected.
Port type	Port type: <ul style="list-style-type: none"> ▪ MAP —The port is a MAP access port. ▪ - (The port is not a MAP access port.)
PoE config	PoE state: <ul style="list-style-type: none"> ▪ enabled ▪ disabled
PoE Draw	Power draw on the port, in watts. For 10/100 Ethernet ports on which PoE is disabled, this field displays <i>off</i> . For gigabit Ethernet ports, this field displays <i>invalid</i> , because PoE is not supported on gigabit Ethernet ports. The value <i>overcurrent</i> indicates a PoE problem such as a short in the cable.

See Also

- **set port poe** on page 94

display port status

Displays configuration and status information for ports.

Syntax — `display port status [port-list]`

- *port-list* — List of physical ports. If you do not specify a port list, information is displayed for all ports.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays information for all ports on a WX1200 switch:

```
WX1200# display port status
Port  Name           Admin  Oper   Config   Actual   Type       Media
=====
  1  1                up     up     auto     100/full network    10/100BaseTx
  2  2                up     up     auto     100/full ap         10/100BaseTx
  3  3                up     up     auto     100/full network    10/100BaseTx
  4  4                up     down   auto           network    10/100BaseTx
  5  5                up     down   auto           network    10/100BaseTx
  6  6                up     down   auto           network    10/100BaseTx
  7  7                up     down   auto           network    10/100BaseTx
  8  8                up     down   auto           network    10/100BaseTx
```

Table 13 describes the fields in this display.

Table 13 Output for display port status

Field	Description
Port	Port number.
Name	Port name. If the port does not have a name, the port number is listed.
Admin	Administrative status of the port: <ul style="list-style-type: none"> ▪ up — The port is enabled. ▪ down — The port is disabled.
Oper	Operational status of the port: <ul style="list-style-type: none"> ▪ up — The port is operational. ▪ down — The port is not operational.
Config	Port speed configured on the port: <ul style="list-style-type: none"> ▪ 10 — 10 Mbps. ▪ 100 — 100 Mbps. ▪ 1000 — 1000 Mbps. ▪ auto — The port sets its own speed.
Actual	Speed and operating mode in effect on the port.
Type	Port type: <ul style="list-style-type: none"> ▪ ap — MAP access point port ▪ network — Network port ▪ wa — Wired authentication port

Table 13 Output for display port status (continued)

Field	Description
Media	Link type: 10/100BaseTX — 10/100BASE-T. GBIC — 1000BASE-SX or 1000BASE-LX GBIC. 1000BaseT — 1000BASE-T. No connector — GBIC slot is empty.

See Also

- **clear port type** on page 74
- **set port** on page 89
- **set port name** on page 93
- **set port negotiation** on page 93
- **set port speed** on page 95
- **set port type ap** on page 97
- **set port type wired-auth** on page 100

display port media-type

Displays the enabled interface types on a WX4400 switch's gigabit Ethernet ports.

See Also — **display port media-type** [*port-list*]

- *port-list* — List of physical ports. MSS displays the enabled interface types for all the specified ports.

Defaults — None.

Access — All.

History — Introduced in MSS Version 4.0.

Usage — This command applies only to the WX4400.

Examples — The following command displays the enabled interface types on all four ports of a WX4400 switch:

```
WX4400# display port media-type
Port  Media Type
=====
 1  GBIC
 2  RJ45
 3  GBIC
 4  GBIC
```

Table 14 describes the fields in this display.

Table 14 Output for display port media-type

Field	Description
Port	Port number.
Preference	Preference setting: GBIC—The GBIC (fiber) interface is enabled. RJ45—The RJ-45 (copper) interface is enabled.

See Also

- **clear port media-type** on page 72
- **set port media-type** on page 91

monitor port counters

Displays and continually updates port statistics.

Syntax — `monitor port counters`

```
[octets | packets | receive-errors | transmit-errors |
collisions | receive-etherstats | transmit-etherstats]
```

- **octets** — Displays octet statistics first.
- **packets** — Displays packet statistics first.
- **receive-errors** — Displays errors in received packets first.
- **transmit-errors** — Displays errors in transmitted packets first.
- **collisions** — Displays collision statistics first.
- **receive-etherstats** — Displays Ethernet statistics for received packets first.

- **transmit-etherstats** — Displays Ethernet statistics for transmitted packets first.

Defaults — All types of statistics are displayed for all ports. MSS refreshes the statistics every 5 seconds. This interval cannot be configured. Statistics types are displayed in the following order by default:

- Octets
- Packets
- Receive errors
- Transmit errors
- Collisions
- Receive Ethernet statistics
- Transmit Ethernet statistics

Access — All.

History—Introduced in MSS Version 3.0.

Usage — Each type of statistic is displayed separately. Press the Spacebar to cycle through the displays for each type.

If you use an option to specify a statistic type, the display begins with that statistic type. You can use one statistic option with the command.

Use the keys listed in Table 15 to control the monitor display.

Table 15 Key Controls for Monitor Port Counters Display

Field	Description
Spacebar	Advances to the next statistic type.
Esc	Exits the monitor. MSS stops displaying the statistics and displays a new command prompt.
c	Clears the statistics counters for the currently displayed statistics type. The counters begin incrementing again.

For error reporting, the cyclic redundancy check (CRC) errors include misalignment errors. Jumbo packets with valid CRCs are not counted. A short packet can be reported as a short packet, a CRC error, or an overrun. In some circumstances, the transmitted octets counter might increment a small amount for a port with nothing attached.

Examples — The following command starts the port statistics monitor beginning with octet statistics (the default):

```
WX4400# monitor port counters
```

As soon as you press Enter, MSS clears the window and displays statistics at the top of the window.

```
Port      Status
-----
1 Up
Rx Octets
27965420
Tx Octets
34886544
...
```

To cycle the display to the next set of statistics, press the Spacebar. In this example, packet statistics are displayed next:

```
Port      Status      Rx Unicast      Rx NonUnicast      Tx Unicast      Tx NonUnicast
-----
1 Up
54620      62144      68318      62556
...
```

Table 16 describes the port statistics displayed by each statistics option. The Port and Status fields are displayed for each option.

Table 16 Output for monitor port counters

Statistics Option	Field	Description
Displayed for All Options octets	Port	Port the statistics are displayed for.
	Status	Port status. The status can be Up or Down.
	Rx Octets	Total number of octets received by the port. This number includes octets received in frames that contained errors.
	Tx Octets	Total number of octets received. This number includes octets received in frames that contained errors.

Table 16 Output for monitor port counters (continued)

Statistics Option	Field	Description
packets	Rx Unicast	Number of unicast packets received. This number does not include packets that contain errors.
	Rx NonUnicast	Number of broadcast and multicast packets received. This number does not include packets that contain errors.
	Tx Unicast	Number of unicast packets transmitted. This number does not include packets that contain errors.
	Tx NonUnicast	Number of broadcast and multicast packets transmitted. This number does not include packets that contain errors.
receive-errors	Rx Crc	Number of frames received by the port that had the correct length but contained an invalid frame check sequence (FCS) value. This statistic includes frames with misalignment errors.
	Rx Error	Total number of frames received in which the Physical layer (PHY) detected an error.
	Rx Short	Number of frames received by the port that were fewer than 64 bytes long.
	Rx Overrun	Number of frames received by the port that were valid but were longer than 1518 bytes. This statistic does not include jumbo packets with valid CRCs.
transmit-errors	Tx Crc	Number of frames transmitted by the port that had the correct length but contained an invalid FCS value.
	Tx Short	Number of frames transmitted by the port that were fewer than 64 bytes long.
	Tx Fragment	Total number of frames transmitted that were less than 64 octets long and had invalid CRCs.
	Tx Abort	Total number of frames that had a link pointer parity error.

Table 16 Output for monitor port counters (continued)

Statistics Option	Field	Description
collisions	Single Coll	Total number of frames transmitted that experienced one collision before 64 bytes of the frame were transmitted on the network.
	Multiple Coll	Total number of frames transmitted that experienced more than one collision before 64 bytes of the frame were transmitted on the network.
	Excessive Coll	Total number of frames that experienced more than 16 collisions during transmit attempts. These frames are dropped and not transmitted.
	Total Coll	Best estimate of the total number of collisions on this Ethernet segment.
receive-etherstats	Rx 64	Number of packets received that were 64 bytes long.
	Rx 127	Number of packets received that were from 65 through 127 bytes long.
	Rx 255	Number of packets received that were from 128 through 255 bytes long.
	Rx 511	Number of packets received that were from 256 through 511 bytes long.
	Rx 1023	Number of packets received that were from 512 through 1023 bytes long.
	Rx 1518	Number of packets received that were from 1024 through 1518 bytes long.
transmit-etherstats	Tx 64	Number of packets transmitted that were 64 bytes long.
	Tx 127	Number of packets transmitted that were from 65 through 127 bytes long.
	Tx 255	Number of packets transmitted that were from 128 through 255 bytes long.
	Tx 511	Number of packets transmitted that were from 256 through 511 bytes long.
	Tx 1023	Number of packets transmitted that were from 512 through 1023 bytes long.
	Tx 1518	Number of packets transmitted that were from 1024 through 1518 bytes long.

See Also

- **display port counters** on page 75

reset port

Resets a port by toggling its link state and Power over Ethernet (PoE) state.

Syntax — `reset port port-list`

- `port-list` — List of physical ports. MSS resets all the specified ports.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The reset command disables the port's link and PoE (if applicable) for at least 1 second, then reenables them. This behavior is useful for forcing a MAP access point that is connected to two WX switches to reboot over the link to the other switch.

Examples — The following command resets port 5:

```
WX1200# reset port 5
```

See Also

- **set port** on page 89

set ap

Configures a Distributed MAP for a MAP access point that is indirectly connected to the WX switch through an intermediate Layer 2 or Layer 3 network.



*Before configuring a Distributed MAP, you must use the **set system countrycode** command to set the IEEE 802.11 country-specific regulations on the WX switch. See “set system countrycode” on page 61.*



*For a MAP that is directly connected to the WX switch, use the **set port type ap** command to configure a MAP access port.*

Syntax — `set ap ap-number serial-id serial-ID model {ap2750 | ap3150 | ap3750 | ap7250 | ap8250 | ap8750 | mp-52 | mp-241 | mp-252 | mp-262 | mp-341 | mp-352 | mp-372 | mp-372-CN | mp-37-JP | mp-620} [radiotype {11a | 11b | 11g}]`

- *ap-number* — Number for the Distributed MAP. The range of valid connection numbers depends on the WX switch model:
 - For a WX4400, you can specify a number from 1 to 256.
 - For a WX1200, you can specify a number from 1 to 30.
- **serial-id** *serial-ID* — MAP access point serial ID. The serial ID is listed on the MAP case. To show the serial ID using the CLI, use the **display version details** command.
- **radiotype** **11a** | **11b** | **11g** — Radio type:
 - **11a** — 802.11a
 - **11b** — 802.11b
 - **11g** — 802.11g

This option applies only to single-radio models.

Defaults — The default values are the same as the defaults for the **set port type ap** command.

Access — Enabled.

History — Introduced in MSS Version 3.0. New values for model option added in Version 4.1:

- AP3750
- AP2750
- mp-620

Version 6.0 renamed the **dap** command to **ap**.

Examples — The following command configures Distributed MAP 1 for MAP model AP2750 with serial-ID M9DE48B012F00:

```
WX4400# set ap 1 serial-id M9DE48B012F00 model ap2750
success: change accepted.
```

The following command removes Distributed MAP 1:

```
WX4400# clear ap 1
This will clear specified AP devices.
Would you like to continue? (y/n) [n]y
```


See Also

- **clear ap** on page 70
- **clear port type** on page 74
- **set port type ap** on page 97
- **set system countrycode** on page 61

set port

Administratively disables or reenables a port.

Syntax — `set port {enable | disable} port-list`

- **enable** — Enables the specified ports.
- **disable** — Disables the specified ports.
- *port-list* — List of physical ports. MSS disables or reenables all the specified ports.

Defaults — All ports are enabled.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — A port that is administratively disabled cannot send or receive packets. This command does not affect the link state of the port.

Examples — The following command disables port 6:

```
WX1200# set port disable 6
success: set "disable" on port 6
```

The following command reenables the port:

```
WX1200# set port enable 6
success: set "enable" on port 6
```

See Also

- **reset port** on page 87

set port-group

Configures a load-sharing port group. All ports in the group function as a single logical link.

Syntax — `set port-group name group-name port-list mode {on | off}`

- **name** *group-name* — Alphanumeric string of up to 255 characters, with no spaces.
- **port-list** — List of physical ports. All the ports you specify are configured together as a single logical link.
- **mode** {**on** | **off**} — State of the group. Use **on** to enable the group or **off** to disable the group. The group is enabled by default.

Defaults — Once configured, a group is enabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You can configure up to 8 ports in a port group, in any combination of ports. The port numbers do not need to be contiguous and you can use 10/100 Ethernet ports and gigabit Ethernet ports in the same port group.

After you add a port to a port group, you cannot configure port parameters on the individual port. Instead, change port parameters on the entire group. Specify the group name instead of an individual port name or number in port configuration commands.

To add or remove ports in a group that is already configured, change the mode to off, add or remove the ports, then change the mode to on.

Examples — The following command configures a port group named `server1` containing ports 1 through 5, and enables the link:

```
WX1200# set port-group name server1 1-5 mode on
success: change accepted.
```

The following commands disable the link for port group `server1`, change the list of ports in the group, and reenables the link:

```
WX1200# set port-group name server1 1-5 mode off
success: change accepted.
WX1200# set port-group name server1 1-4,7 mode on
success: change accepted.
```

See Also

- **clear port-group** on page 71
- **display port-group** on page 76

set port media-type Disables the fiber interface and enables the copper interface on an WX4400 gigabit Ethernet port.

Syntax — `set port media-type port-list rj45`

- *port-list*—List of physical ports. MSS sets the preference on all the specified ports.
- *rj45*—Uses the copper interface.

Defaults — The GBIC (fiber) interface is enabled, and the copper interface is disabled, by default.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — This command applies only to the WX4400.

If you set the port interface to RJ-45 on a port that already has an active fiber link, MSS immediately changes the link to the copper interface.

Examples — The following command disables the fiber interface and enables the copper interface on port 2:

```
WX4400# set port media-type 2 rj45
```

See Also

- **clear port media-type** on page 72
- **display port media-type** on page 81

set port mirror

Configures port mirroring. Port mirroring is a troubleshooting feature that copies (mirrors) traffic sent or received by a WX port (the source port) to another port (the observer) on the same WX. You can attach a protocol analyzer to the observer port to examine the source port's traffic. Both traffic directions (send and receive) are mirrored.

Syntax — `set port mirror source-port observer observer-port`

- *source-port* — Number of the port whose traffic you want to analyze. You can specify only one port.
- *observer-port* — Number of the port to which you want the switch to copy the source port's traffic.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — The switch can have one port mirroring pair (one source port and one observer port) at a time. The source port can be a network port, MAP access port, or wired authentication port. However, the observer port must be a network port, and cannot be a member of any VLAN or port group.

Examples — The following command sets port 2 to monitor port 1's traffic:

```
WX4400# set port 1 observer 2
```

See Also

- **clear port name** on page 72
- **display port status** on page 79

set port name

Assigns a name to a port. After naming a port, you can use the port name or number in other CLI commands.

Syntax — `set port port name name`

- *port* — Number of a physical port. You can specify only one port.
- **name** *name* — Alphanumeric string of up to 16 characters, with no spaces.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To simplify configuration and avoid confusion between a port's number and its name, 3Com recommends that you do not use numbers as port names.

Examples — The following command sets the name of port 7 to *adminpool*:

```
WX1200# set port 7 name adminpool
success: change accepted.
```

See Also

- **clear port name** on page 72
- **display port status** on page 79

set port negotiation

Disables or reenables autonegotiation on gigabit Ethernet or 10/100 Ethernet ports.

Syntax — `set port negotiation port-list {enable | disable}`

- *port-list* — List of physical ports. MSS disables or reenables autonegotiation on all the specified ports.
- **enable** — Enables autonegotiation on the specified ports.
- **disable** — Disables autonegotiation on the specified ports.

Defaults — Autonegotiation is enabled on all Ethernet ports by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — WX1200 10/100 Ethernet ports support half-duplex and full-duplex operation.

3Com recommends that you do not configure the mode of an WX port so that one side of the link is set to autonegotiation while the other side is set to full-duplex. Although MSS allows this configuration, it can result in slow throughput on the link. The slow throughput occurs because the side that is configured for autonegotiation falls back to half-duplex. A stream of large packets sent to an WX port in such a configuration can cause forwarding on the link to stop.

Examples — The following command disables autonegotiation on ports 3 and 5:

```
WX1200# set port negotiation 3,5 disable
```

The following command enables autonegotiation on port 2:

```
WX1200# set port negotiation 2 enable
```

set port poe

Enables or disables Power over Ethernet (PoE) on ports connected to MAP access points.



CAUTION: *When you set the port type for MAP use, you can enable PoE on the port. Use the WX switch's PoE to power 3Com MAP access points only. If you enable PoE on ports connected to other devices, damage can result.*

Syntax — `set ap <apnum> port <portnum> model <ap_type> poe enable | disable`

- **enable** — Enables PoE on the specified ports.
- **disable** — Disables PoE on the specified ports.

Defaults — PoE is disabled on network and wired authentication ports. The state on MAP access point ports depends on whether you enabled or disabled PoE when setting the port type. See **set port type ap** on page 97.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command does not apply to any gigabit Ethernet ports or to ports 7 and 8 on the WX1200 switch.

Examples — The following command disables PoE on ports 4 and 5, which are connected to a MAP access point:

```
WX1200# set port poe 4,5 disable
```

If you are enabling power on these ports, they must be connected only to approved PoE devices with the correct wiring. Do you wish to continue? (y/n) [n]y

The following command enables PoE on ports 4 and 5:

```
WX1200# set port poe 4,5 enable
```

If you are enabling power on these ports, they must be connected only to approved PoE devices with the correct wiring. Do you wish to continue? (y/n) [n]y

See Also

- **set port type ap** on page 97
- **set port type wired-auth** on page 100

set port speed

Changes the speed of a port.

Syntax — `set port speed port-list {10 | 100 | 1000 | auto}`

- *port-list* — List of physical ports. MSS sets the port speed on all the specified ports.
- **10** — Sets the port speed of a 10/100 Ethernet port to 10 Mbps and sets the operating mode to full-duplex.
- **100** — Sets the port speed of a 10/100 Ethernet port to 100 Mbps and sets the operating mode to full-duplex.
- **1000** — Sets the port speed of a gigabit Ethernet port to 1000 Mbps and sets the operating mode to full-duplex.
- **auto** — Enables a port to detect the speed and operating mode of the traffic on the link and set itself accordingly.

Defaults — All ports are set to auto.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — 3Com recommends that you do not configure the mode of a WX port so that one side of the link is set to autonegotiation while the other side is set to full-duplex. Although MSS allows this configuration, it can result in slow throughput on the link. The slow throughput occurs because the side that is configured for autonegotiation falls back to half-duplex. A stream of large packets sent to an WX port in such a configuration can cause forwarding on the link to stop.

Examples — The following command sets the port speed on ports 1 and 3 through 4 to 10 Mbps and sets the operating mode to full-duplex:

```
WX1200# set port speed 1,3-4 10
```

set port trap

Enables or disables Simple Network Management Protocol (SNMP) linkup and linkdown traps on an individual port.

Syntax — `set port trap port-list {enable | disable}`

- *port-list* — List of physical ports.
- **enable** — Enables the Telnet server.
- **disable** — Disables the Telnet server.

Defaults — SNMP linkup and linkdown traps are disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The **set port trap** command overrides the global setting of the **set snmp trap** command.

The **set port type** command does not affect the global trap information displayed by the **display snmp configuration** command. For example, if you globally enable linkup and linkdown traps but then disable the traps on a single port, the **display snmp configuration** command still indicates that the traps are globally enabled.

Examples — The following command enables SNMP linkup and linkdown traps on ports 3 and 4:

```
WX1200# set port trap 3-4 enable
```


See Also

- **set ip snmp server** on page 180
- **set snmp community** on page 185

set port type ap

Configures an WX switch port for a MAP access point.



CAUTION: When you set the port type for MAP use, you must specify the PoE state (enable or disable) of the port. Use the WX switch's PoE to power 3Com MAP access points only. If you enable PoE on a port connected to another device, physical damage to the device can result.



Before configuring a port as a MAP access point port, you must use the **set system countrycode** command to set the IEEE 802.11 country-specific regulations on the WX switch. See "set system countrycode" on page 61.



For a MAP that is indirectly connected to the WX switch through an intermediate Layer 2 or Layer 3 network, use the **set ap** command to configure a Distributed MAP.



Before changing the port type from **ap** to **wired-auth** or from **wired-auth** to **ap**, you must reset the port with the clear port type command.

Syntax — `set port type ap port-list model {ap2750 | ap3150 | ap3750 | ap7250 | ap8250 | ap8750 | mp-52 | mp-241 | mp-252 | mp-262 | mp-341 | mp-352 | mp-372 | mp-372-CN | mp-37-JP | mp-620}`

`poe {enable | disable}`

`[radiotype {11a | 11b | 11g}]`

- *port-list* — List of physical ports.
- `model {ap2750 | ap3150 | ap3750 | ap7250 | ap8250 | ap8750 | mp-52 | mp-241 | mp-252 | mp-262 | mp-341 | mp-352 | mp-372 | mp-372-CN | mp-37-JP | mp-620}` — MAP access point model:
- `poe enable | disable` — Power over Ethernet (PoE) state.
- `radiotype 11a | 11b | 11g` — Radio type:
 - 11a — 802.11a
 - 11b — 802.11b
 - 11g — 802.11g

Defaults — All WX ports are network ports by default.

MAP access point models AP2750, MAP-241, and MAP-341 have a single radio that can be configured for 802.11a or 802.11b/g. Other MAP models have two radios. On two-radio models, one radio is always 802.11a. The other radio is 802.11b/g, but can be configured for 802.11b or 802.11g exclusively. If the country of operation specified by the set system countrycode command does not allow 802.11g, the default is 802.11b.

The radios in models MAP-620 require external antennas, and model MAP-262 requires an external antenna for the 802.11b/g radio. The following models have internal antennas but also have connectors for optional use of external antennas instead: AP2750, AP3150, AP3750, AP7250, AP8250, AP8750, MAP-372, MAP-372-CN, and MAP-372-JP. (Antenna support on a specific model is limited to the antennas certified for use with that model.) To specify the antenna model, use the **set ap radio antennatype** command.

Access — Enabled.

History — Introduced in MSS Version 3.0. New values for model options AP3750, AP2750 added in Version 4.1. New value for model option AP3150 added in Version 6.0.

Usage — You cannot set a port type if the port is a member of a port VLAN. To remove a port from a VLAN, use the **clear vlan** command. To reset a port as a network port, use the **clear port type** command.

When you change port type, MSS applies default settings appropriate for the port type. Table 17 lists the default settings that MSS applies when you set a port's type to **ap**.

Table 17 MAP Access Port Defaults

Port Parameter	Setting
VLAN membership	Removed from all VLANs. You cannot assign a MAP access port to a VLAN. MSS automatically assigns MAP access ports to VLANs based on user traffic.
Spanning Tree Protocol (STP)	Not applicable
802.1X	Uses authentication parameters configured for users.

Table 17 MAP Access Port Defaults (continued)

Port groups	Not applicable
IGMP snooping	Enabled as users are authenticated and join VLANs.
Maximum user sessions	Not applicable

This command does not apply to any gigabit Ethernet ports or to ports 7 and 8 on the WX1200 switch or port 3 on the WX2200 switch.

To manage a MAP access point on a switch model that does not have 10/100 Ethernet ports, use the **set ap** command to configure a Distributed MAP connection on the switch.

Examples — The following command sets ports 1 through 3 and port 5 for MAP access point model AP2750 and enables PoE on the ports:

```
WX1200# set port type ap 1-3,5 model ap2750 poe enable
This may affect the power applied on the configured ports.
Would you like to continue? (y/n) [n]y
```

The following command sets ports 1 through 3 and port 5 for MAP access point model AP7250 and enables PoE on the ports:

```
WX1200# set port type ap 1-3,5 model ap7250 poe enable
This may affect the power applied on the configured ports.
Would you like to continue? (y/n) [n]y
```

The following command sets ports 1 through 3 and port 5 for MAP access point model AP8250 and enables PoE on the ports:

```
WX1200# set port type ap 1-3,5 model ap8250 poe enable
This may affect the power applied on the configured ports.
Would you like to continue? (y/n) [n]y
```

The following command sets ports 1 through 3 and port 5 for MAP access point model AP8750 and enables PoE on the ports:

```
WX1200# set port type ap 1-3,5 model ap8750 poe enable
This may affect the power applied on the configured ports.
Would you like to continue? (y/n) [n]y
```

The following command resets port 5 by clearing it:

```
WX1200# clear port type 5
This may disrupt currently authenticated users.
Are you sure? (y/n) [n]y
success: change accepted.
```

See Also

- **clear ap** on page 70
- **clear port type** on page 74
- **set ap radio antennatype** on page 383
- **set ap** on page 87
- **set port type wired-auth** on page 100
- **set system countrycode** on page 61

**set port type
wired-auth**


Configures a WX switch port for a wired authentication user.

*Before changing the port type from **ap** to **wired-auth** or from **wired-auth** to **ap**, you must reset the port with the **clear port type** command.*

Syntax — `set port type wired-auth port-list [tag tag-list] [max-sessions num] [auth-fall-thru {last-resort | none | web-portal}]`

- *port-list* — List of physical ports.
- *tag-list* — One or more numbers between 1 and 4094 that subdivide a wired authentication port into virtual ports.
- *num* — Maximum number of simultaneous user sessions supported.
- **last-resort** — Automatically authenticates the user, without requiring a username and password.
- **none** — Denies authentication and prohibits the user from accessing the network over this port.
- **web-portal** — Serves the user a web page from the WX switch's nonvolatile storage for secure login to the network.

Defaults — The default tag-list is null (no tag values). The default number of sessions is 1. The default fallthru authentication type is none.

Access — Enabled.

History—Introduced in MSS Version 3.0. Option for WebAAA fallthru authentication type changed from **web-auth** to **web-portal** in MSS Version 4.0.

Usage — You cannot set a port's type if the port is a member of a port VLAN. To remove a port from a VLAN, use the **clear vlan** command. To reset a port as a network port, use the **clear port type** command.

When you change port type, MSS applies default settings appropriate for the port type. Table 18 lists the default settings that MSS applies when you set a port's type to **ap**.

Table 18 Wired Authentication Port Details

Port Parameter	Setting
VLAN membership	Removed from all VLANs. You cannot assign a MAP access port to a VLAN. MSS automatically assigns MAP access ports to VLANs based on user traffic.
Spanning Tree Protocol (STP)	Not applicable
802.1X	Uses authentication parameters configured for users.
Port groups	Not applicable
IGMP snooping	Enabled as users are authenticated and join VLANs.
Maximum user sessions	1 (one).
Falldthru authentication type	None

For 802.1X clients, wired authentication works only if the clients are directly attached to the wired authentication port, or are attached through a hub that does not block forwarding of packets from the client to the PAE group address (01:80:c2:00:00:03).

Wired authentication works in accordance with the 802.1X specification, which prohibits a client from sending traffic directly to an authenticator's MAC address until the client is authenticated. Instead of sending traffic to the authenticator's MAC address, the client sends packets to the PAE group address.

The 802.1X specification prohibits networking devices from forwarding PAE group address packets, because this would make it possible for multiple authenticators to acquire the same client.

For non-802.1X clients, who use MAC authentication, WebAAA, or last-resort authentication, wired authentication works if the clients are directly attached or indirectly attached.

Examples — The following command sets port 2 for a wired authentication user:

```
WX1200# set port type wired-auth 2
success: change accepted
```

The following command sets port 7 for a wired authentication user and specifies a maximum of three simultaneous user sessions:

```
WX1200# set port type wired-auth 7 max-sessions 3
success: change accepted
```

See Also

- **clear port type** on page 74
- **set port type ap** on page 97

5

VLAN COMMANDS

Use virtual LAN (VLAN) commands to configure and manage parameters for individual port VLANs on network ports, and to display information about clients roaming within a mobility domain.

Commands by usage

This chapter presents VLAN commands alphabetically. Use Table 19 to locate commands in this chapter based on their use.

Table 19 VLAN Commands by Usage

Type	Command
Creation	set security l2-restrict on page 123
Ports	set vlan port on page 125
	clear security 12-restrict on page 105
	display vlan config on page 118
Roaming and Tunnels	display roaming station on page 113
	display roaming vlan on page 115
	display security 12-restrict on page 116
Restriction of Client	set security l2-restrict on page 123
Layer 2 Forwarding	display security 12-restrict on page 116
	clear security 12-restrict on page 105
	clear security 12-restrict counters on page 106
Tunnel Affinity	set vlan tunnel-affinity on page 126
FDB Entries	set fdb on page 121
	display fdb on page 109
	display fdb count on page 112
	clear fdb on page 104
FDB Aging Timeout	set fdb agingtime on page 122

Table 19 VLAN Commands by Usage (continued)

Type	Command
	display fdb agingtime on page 111
VLAN Profiles for MAP local Switching	clear vlan-profile on page 108
	clear vlan-profile on page 108
	display vlan-profile on page 120
	set vlan profile on page 127

clear fdb

Deletes an entry from the forwarding database (FDB).

Syntax — `clear fdb {perm | static | dynamic | port port-list} [vlan vlan-id] [tag tag-value]`

- **perm** — Clears permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle. You must specify a VLAN name or number with this option.
- **static** — Clears static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle. You must specify a VLAN name or number with this option.
- **dynamic** — Clears dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle. You are not required to specify a VLAN name or number with this option.
- **port *port-list*** — Clears dynamic entries that match destination ports in the port list. You are not required to specify a VLAN name or number with this option.
- **vlan *vlan-id*** — VLAN name or number—required for removing permanent and static entries. For dynamic entries, specifying a VLAN removes entries that match only that VLAN. Otherwise, dynamic entries that match all VLANs are removed.
- **tag *tag-value*** — VLAN tag value that identifies a virtual port. If you do not specify a tag value, MSS deletes only entries that match untagged interfaces. Specifying a tag value deletes entries that match only the specified tagged interfaces

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You can delete forwarding database entries based on entry type, port, or VLAN. A VLAN name or number is required for deleting permanent or static entries.

Examples — The following command clears all static forwarding database entries that match VLAN *blue*:

```
WX4400# clear fdb static vlan blue
success: change accepted.
```

The following command clears all dynamic forwarding database entries that match all VLANs:

```
WX4400# clear fdb dynamic
success: change accepted.
```

The following command clears all dynamic forwarding database entries that match ports 3 and 5:

```
WX4400# clear fdb port 3,5
success: change accepted.
```

See Also

- **display fdb** on page 109
- **set fdb** on page 121

clear security 12-restrict

Removes one or more MAC addresses from the list of destination MAC addresses to which clients in a VLAN are allowed to send traffic at Layer 2.

Syntax — `clear security 12-restrict vlan vlan-id [permit-mac mac-addr [mac-addr] | all]`

- *vlan-id* — VLAN name or number.
- **permit-mac** — List of MAC addresses. MSS no longer allows clients *mac-addr* in the VLAN to send traffic to the MAC addresses at [*mac-addr*] Layer 2.
- **all** — Removes all MAC addresses from the list.

Defaults — If you do not specify a list of MAC addresses or **all**, all addresses are removed.

Access — Enabled.

History —Introduced in MSS Version 4.1.

Usage — If you clear all MAC addresses, Layer 2 forwarding is no longer restricted in the VLAN. Clients within the VLAN will be able to communicate directly.

To clear the statistics counters without removing any MAC addresses, use the **clear security 12-restrict counters** command instead.

Examples — The following command removes MAC address aa:bb:cc:dd:ee:ff from the list of addresses to which clients in VLAN *abc_air* are allowed to send traffic at Layer 2:

```
WX4400# clear security 12-restrict vlan abc_air permit-mac
aa:bb:cc:dd:ee:ff
success: change accepted.
```

See Also

- **clear security 12-restrict counters** on page 106
- **clear security 12-restrict** on page 105
- **display security 12-restrict** on page 116

clear security 12-restrict counters

Clears statistics counters for Layer 2 forwarding restriction.

Syntax — **clear security 12-restrict counters** [**vlan** *vlan-id* | **all**]

- *vlan-id* — VLAN name or number.
- **all** — Clears Layer 2 forwarding restriction counters for all VLANs.

Defaults — If you do not specify a VLAN or **all**, counters for all VLANs are cleared.

Access — Enabled.

History —Introduced in MSS Version 4.1.

Usage — To clear MAC addresses from the list of addresses to which clients are allowed to send data, use the **clear security 12-restrict** command instead.

Examples — The following command clears Layer 2 forwarding restriction statistics for VLAN *abc_air*:

```
WX4400# clear security 12-restrict counters vlan abc_air
success: change accepted.
```

See Also

- **clear security 12-restrict** on page 105
- **set security 12-restrict** on page 123
- **display security 12-restrict** on page 116

clear vlan

Removes physical or virtual ports from a VLAN or removes a VLAN entirely.



CAUTION: *When you remove a VLAN, MSS completely removes the VLAN from the configuration and also removes all configuration information that uses the VLAN. If you want to remove only a specific port from the VLAN, make sure you specify the port number in the command.*

Syntax — `clear vlan vlan-id [port port-list [tag tag-value]]`

- *vlan-id* — VLAN name or number.
- **port** *port-list* — List of physical ports. MSS removes the specified ports from the VLAN. If you do not specify a list of ports, MSS removes the VLAN entirely.
- **tag** *tag-value* — Tag number that identifies a virtual port. MSS removes only the specified virtual port from the specified physical ports.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — If you do not specify a *port-list*, the entire VLAN is removed from the configuration.



*You cannot delete the default VLAN but you can remove ports from it. To remove ports from the default VLAN, use the **port** port-list option.*

Examples — The following command removes port 1 from VLAN *green*:

```
WX4400# clear vlan green port 1
This may disrupt user connectivity.
Do you wish to continue? (y/n) [n]y
success: change accepted.
```

The following command removes port 4, which uses tag value 69, from VLAN *red*:

```
WX1200# clear vlan red port 4 tag 69
This may disrupt user connectivity.
Do you wish to continue? (y/n) [n]y
success: change accepted.
```

The following command completely removes VLAN *marigold*:

```
WX4400# clear vlan marigold
This may disrupt user connectivity.
Do you wish to continue? (y/n) [n]y
success: change accepted.
```

See Also

- **set vlan port** on page 125
- **display vlan config** on page 118

clear vlan-profile

Removes a VLAN profile or individual entries from a VLAN profile.

Syntax — `clear vlan-profile profile-name [vlan vlan-name]`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — A VLAN profile lists the VLANs for which traffic is locally switched by MAPs where the VLAN profile is applied. Use this command to remove individual VLANs from a VLAN profile, or to remove an entire VLAN profile. If you remove all of the entries from a VLAN profile, the VLAN profile itself is removed.

- **profile-name**—VLAN profile name
- **vlan-name**—Name of a VLAN to remove from the VLAN profile.

If a VLAN profile is changed so that traffic that had been tunneled to an VX switch is now locally switched by MAPs, or vice-versa, the sessions of clients associated with the MAPs where the VLAN profile is applied are terminated, and the clients must re-associate with the MAPs.

Examples — The following command removes the entry for VLAN *red* from VLAN profile *locals*:

```
WX# clear vlan-profile locals vlan red
WX#
```

The following command removes VLAN profile *locals*:

```
WX# clear vlan-profile locals
WX#
```

See Also

- **display vlan-profile** on page 120
- **set ap local-switching vlan-profile** on page 380
- **set vlan profile** on page 127
- **display vlan-profile** on page 120

display fdb

Displays entries in the forwarding database.

Syntax — `display fdb [mac-addr-glob [vlan vlan-id]]`
`display fdb {perm | static | dynamic | system | all} [port`
`port-list | vlan vlan-id]`

- *mac-addr-glob* — A single MAC address or set of MAC addresses. Specify a MAC address, or use the wildcard character (*) to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 31.)
- `vlan vlan-id` — Name or number of a VLAN for which to display entries.
- **perm** — Displays permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
- **static** — Displays static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.

- **dynamic** — Displays dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle.
- **system** — Displays system entries. A system entry is added by MSS. For example, the authentication protocols can add entries for wired and wireless authentication users.
- **all** — Displays all entries in the database, or all the entries that match a particular port or ports or a particular VLAN.
- **port *port-list*** — Destination port(s) for which to display entries.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Usage — To display the entire forwarding database, enter the **display fdb** command without options. To display only a portion of the database, use optional parameters to specify the types of entries you want to display.

Examples — The following command displays all entries in the forwarding database:

```
WX4400# display fdb all
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN TAG  Dest MAC/Route Des [CoS]  Destination Ports      [Protocol Type]
-----
  1       00:01:97:13:0b:1f          1                      [ALL]
  1       aa:bb:cc:dd:ee:ff          *                       3                      [ALL]
  1       00:0b:0e:02:76:f5          1                      [ALL]
Total Matching FDB Entries Displayed = 3
```

The top line of the display identifies the characters to distinguish among the entry types.

The following command displays all entries that begin with the MAC address glob 00:

```
WX4400# display fdb 00:*
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN TAG  Dest MAC/Route Des [CoS]  Destination Ports      [Protocol Type]
-----
  1       00:01:97:13:0b:1f          1                      [ALL]
  1       00:0b:0e:02:76:f5          1                      [ALL]
Total Matching FDB Entries Displayed = 2
```

Table 20 describes the fields in the **display fdb** output.

Table 20 Output for display fdb

Field	Description
VLAN	VLAN number.
TAG	VLAN tag value. If the interface is untagged, the TAG field is blank.
Dest MAC/Route Des	MAC address of this forwarding entry's destination.
CoS	Type of entry. The entry types are explained in the first row of the command output. Note: This Class of Service (CoS) value is not associated with MSS quality of service (QoS) features.
Destination Ports	Wireless LAN switch port associated with the entry. A WX switch sends traffic to the destination MAC address through this port.
Protocol Type	Layer 3 protocol address types that can be mapped to this entry.
Total Matching FDB Entries Displayed	Number of entries displayed by the command.

See Also

- **clear fdb** on page 104
- **set fdb** on page 121

display fdb agingtime

Displays the aging timeout period for forwarding database entries.

Syntax — `display fdb agingtime [vlan vlan-id]`

- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, the aging timeout period for each VLAN is displayed.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays the aging timeout period for all VLANs:

```
WX1200# display fdb agingtime
```

```
VLAN 2 aging time = 600 sec
VLAN 1 aging time = 300 sec
```

Because the forwarding database aging timeout period can be configured only on an individual VLAN basis, the command lists the aging timeout period for each VLAN separately.

See Also

- **set fdb agingtime** on page 122

display fdb count

Lists the number of entries in the forwarding database.

Syntax — `display fdb count {perm | static | dynamic}`
`[vlan vlan-id]`

- **perm** — Lists the number of permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
- **static** — Lists the number of static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.
- **dynamic** — Lists the number of dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle.
- **vlan vlan-id** — VLAN name or number. Entries are listed for only the specified VLAN.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

The following command lists the number of dynamic entries that the forwarding database contains:

```
WX1200# display fdb count dynamic
Total Matching Entries = 2
```

See Also

- **display fdb** on page 109

display roaming station

Shows a list of the stations roaming to the wireless LAN switch through a VLAN tunnel.

Syntax — display roaming station

[**vlan** *vlan-id*] [**peer** *ip-addr*]

- **vlan** *vlan-id* — Output is restricted to stations using this VLAN.
- **peer** *ip-addr* — Output is restricted to stations tunnelling through this peer WX switch in the Mobility Domain.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. Old AP MAC field removed in MSS Version 4.1.

Usage — The output displays roaming stations within the previous 1 second.

Examples — To display all stations roaming to the WX switch, type the following command:

```
WX4400# display roaming station
User Name           Station Address      VLAN      State
-----
redsq               10.10.10.5          violet    Up
```

Table 21 describes the fields in the display.

Table 21 Output for display roaming station

Field	Description
User Name	Name of the user. This is the name used for authentication. The name resides in a RADIUS server database or the local user database on a wireless LAN switch.
Station Address	IP address of the user device.
VLAN	Name of the VLAN to which the RADIUS server or WX switch local user database assigned the user.

Table 21 Output for display roaming station (continued)

Field	Description
State	State of the session: <ul style="list-style-type: none"> <li data-bbox="596 348 1253 453">▪ Setup — Station is attempting to roam to this WX switch. This switch has asked the WX from which the station is roaming for the station's session information and is waiting for a reply. <li data-bbox="596 470 1253 539">▪ Up — MSS has established a tunnel between the WX switches and the station has successfully roamed to this WX over the tunnel. <li data-bbox="596 557 1253 626">▪ Chck — This WX switch is in the process of accepting a reassociation request from the roaming peer WX switch for a station currently roaming to the peer switch. <li data-bbox="596 644 1253 713">▪ TChck — This WX switch is in the process of accepting a reassociation request from the roaming peer WX switch for a station currently roaming to this switch. <li data-bbox="596 730 1253 800">▪ WInd — This WX switch is waiting for network congestion to clear before sending the roaming indication to the roaming peer WX switch. <li data-bbox="596 817 1253 887">▪ WResp — This WX switch is waiting for network congestion to clear before sending the roaming response to the roaming peer WX switch.

See Also

- **display roaming vlan** on page 115

**display roaming
vlan**

Shows all VLANs in the mobility domain, the WX switches servicing the VLANs, and their tunnel affinity values configured on each switch for the VLANs.

Syntax — `display roaming vlan`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command shows the current roaming VLANs:

```
WX4400# display roaming vlan
VLAN                WX                Affinity
-----
vlan-cs             192.168.14.2      5
vlan-eng            192.168.14.4      5
vlan-fin            192.168.14.2      5
vlan-it             192.168.14.4      5
vlan-it             192.168.14.2      5
vlan-pm             192.168.14.2      5
vlan-sm             192.168.14.2      5
vlan-tp             192.168.14.4      5
vlan-tp             192.168.14.2      5
```

Table 22 describes the fields in the display.

Table 22 Output for display roaming vlan

Field	Description
VLAN	VLAN name.
WX	System IP address of the wireless LAN switch on which the VLAN is configured.
Affinity	Preference of this WX switch for forwarding user traffic for the VLAN. A higher number indicates a greater preference.

See Also

- **display roaming station** on page 113
- **display vlan config** on page 118

**display security
12-restrict**

Displays configuration information and statistics for Layer 2 forwarding restriction.

Syntax — `display security 12-restrict [vlan vlan-id / all]`

vlan-id — VLAN name or number.

all — Displays information for all VLANs.

Defaults — If you do not specify a VLAN name or **all**, information is displayed for all VLANs.

Access — Enabled.

History — Introduced in MSS Version 4.1.

Examples — The following command shows Layer 2 forwarding restriction information for all VLANs:

VLAN Name	En Drops	Permit MAC	Hits
1 default	Y	0 00:0b:0e:02:53:3e 00:30:b6:3e:5c:a8	5947 9
2 vlan-2	Y	0 04:04:04:04:04:04	0

Table 23 describes the fields in the display.

Table 23 Output for display security 12-restrict

Field	Description
VLAN	VLAN number.
Name	VLAN name.
En	Enabled state of the feature for the VLAN: <ul style="list-style-type: none"> ■ Y — Enabled. Forwarding of Layer 2 traffic from clients is restricted to the MAC address(es) listed under Permit MAC. ■ N — Disabled. Layer 2 forwarding is not restricted.
Drops	Number of packets dropped because the destination MAC address was not one of the addresses listed under Permit MAC.
Permit MAC	MAC addresses to which clients in the VLAN are allowed to send traffic at Layer 2.

Table 23 Output for display security 12-restrict

Field	Description
Hits	Number of packets whose source MAC address was a client in this VLAN, and whose destination MAC address was one of those listed under Permit MAC.

See Also

- **clear security 12-restrict** on page 105
- **clear security 12-restrict counters** on page 106
- **set security 12-restrict** on page 123

display tunnel

Shows the tunnels from the wireless LAN switch where you type the command.

Syntax — `display tunnel`

Defaults — None.

Access — Enabled

History — Introduced in MSS Version 3.0.

Examples — To display all tunnels from a WX switch to other WX switches in the Mobility Domain, type the following command.

```
WX4400# display tunnel
VLAN          Local Address  Remote Address  State   Port  LVID  RVID
-----
vlan-eng      192.168.14.2   192.168.14.4   DORMANT 1024  4096  130
```

Table 24 describes the fields in the display.

Table 24 Output for display tunnel

Field	Description
VLAN	VLAN name.
Local Address	IP address of the local end of the tunnel. This is the system IP address of the wireless access switch where you enter the command.

Table 24 Output for display tunnel (continued)

Field	Description
Remote Address	IP address of the remote end of the tunnel. This is the system IP address of another WX switch in the mobility domain.
State	Tunnel state: <ul style="list-style-type: none"> ▪ Up ▪ Dormant
Port	Tunnel port ID.
LVID	Local VLAN ID.
RVID	Remote VLAN ID.

See Also

- **display vlan config** on page 118

display vlan config

Shows VLAN information.

Syntax — `display vlan config [vlan-id]`

- *vlan-id* — VLAN name or number. If you do not specify a VLAN, information for all VLANs is displayed.

Defaults — None.**Access** — All.**History** — Introduced in MSS Version 3.0.**Examples** — The following command displays information for VLAN *burgundy*:

```
WX1200# display vlan config burgundy
VLAN Name      Admin  VLAN  Tunl      Port
Status  State Affin  Port      Tag  State
-----
   2 burgundy   Up    Up      5
                        2      none Up
                        3      none Up
                        4      none Up
                        6      none Up
4094 web-aaa   Up    Up      0
                        2      4094 Up
                        t:10.10.40.4 none Up
```

Table 25 describes the fields in this display.

Table 25 Output for display vlan config

Field	Description
VLAN	VLAN number.
Name	VLAN name.
Admin Status	Administrative status of the VLAN: <ul style="list-style-type: none"> ▪ Down — The VLAN is disabled. ▪ Up — The VLAN is enabled.
VLAN State	Link status of the VLAN: <ul style="list-style-type: none"> ▪ Down — The VLAN is not connected. ▪ Up — The VLAN is connected.
Tunl Affin	Tunnel affinity value assigned to the VLAN.
Port	Member port of the VLAN. The port can be a physical port or a virtual port. <ul style="list-style-type: none"> ▪ Physical ports are 10/100 Ethernet or gigabit Ethernet ports on the WX switch, and are listed by port number. ▪ Virtual ports are tunnels to other WX switches in a mobility domain, and are listed as follows: <i>t:ip-addr</i>, where <i>ip-addr</i> is the system IP address of the WX switch at the other end of the tunnel. <p>Note: This field can include MAP access ports and wired authentication ports, because MSS dynamically adds these ports to a VLAN when handling user traffic for the VLAN.</p>
Tag	Tag value assigned to the port.
Port State	Link state of the port: <ul style="list-style-type: none"> ▪ Down — The port is not connected. ▪ Up — The port is connected.

See Also

- **clear security 12-restrict** on page 105
- **set security 12-restrict** on page 123
- **set vlan port** on page 125
- **set vlan tunnel-affinity** on page 126

display vlan-profile Displays the contents of the VLAN profiles configured on the WX switch. A VLAN profile lists the VLANs for which traffic is locally switched by MAPs where the VLAN profile is applied.

Syntax — **display vlan-profile** [*profile-name*]

- *profile-name* —VLAN profile name

Defaults — If a *profile-name* is not specified, the contents of all VLAN profiles configured on the WX switch are displayed.

Access — All.

History — Introduced in MSS Version 6.0.

Examples — The following command displays the contents of VLAN profile *locals*:

```
WX# display vlan-profile locals
vlan-profile: locals
Vlan Name      Tag
-----
blue           none
red            45
ap numbers: 67
```

Table 26 describes the fields in the **display vlan-profile** output.

Table 26 Output for display vlan-profile

Field	Description
vlan-profile	Name of the VLAN profile.
Vlan Name	Name of the VLAN for which local switching is performed.
Mode	Value of the 802.1Q tag used for the VLAN.
ap numbers	The index numbers of the APs where this VLAN profile is applied.

See Also

- **clear vlan-profile** on page 108
- **set ap local-switching vlan-profile** on page 380
- **set vlan profile** on page 127

set fdb

Adds a permanent or static entry to the forwarding database.

Syntax — `set fdb {perm | static}`

`mac-addr port port-list vlan vlan-id [tag tag-value]`

- **perm** — Adds a permanent entry. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
- **static** — Adds a static entry. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.
- `mac-addr` — Destination MAC address of the entry. Use colons to separate the octets (for example, 00:11:22:aa:bb:cc).
- `port port-list` — List of physical destination ports for which to add the entry. A separate entry is added for each port you specify.
- `vlan vlan-id` — Name or number of a VLAN of which the port is a member. The entry is added only for the specified VLAN.
- `tag tag-value` — VLAN tag value that identifies a virtual port. You can specify a number from 1 through 4095. If you do not specify a tag value, an entry is created for an untagged interface only. If you specify a tag value, an entry is created only for the specified tagged interface.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You cannot add a multicast or broadcast address as a permanent or static FDB entry.

Examples — The following command adds a permanent entry for MAC address 00:11:22:aa:bb:cc on ports 3 and 5 in VLAN *blue*:

```
WX1200# set fdb perm 00:11:22:aa:bb:cc port 3,5 vlan blue
success: change accepted.
```

The following command adds a static entry for MAC address 00:2b:3c:4d:5e:6f on port 1 in the *default* VLAN:

```
WX4400# set fdb static 00:2b:3c:4d:5e:6f port 1 vlan default
success: change accepted.
```

See Also

- **clear fdb** on page 104
- **display fdb** on page 109

set fdb agingtime

Changes the aging timeout period for dynamic entries in the forwarding database.

Syntax — `set fdb agingtime vlan-id age seconds`

- *vlan-id* — VLAN name or number. The timeout period change applies only to entries that match the specified VLAN.
- *age seconds* — Value for the timeout period, in seconds. You can specify a value from 0 through 1,000,000. If you change the timeout period to 0, aging is disabled.

Defaults — The aging timeout period is 300 seconds (5 minutes).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command changes the aging timeout period to 600 seconds for entries that match VLAN *orange*:

```
WX4400# set fdb agingtime orange age 600
success: change accepted.
```

See Also

- **display fdb agingtime** on page 111

set security l2-restrict

Restricts Layer 2 forwarding between clients in the same VLAN. When you restrict Layer 2 forwarding in a VLAN, MSS allows Layer 2 forwarding only between a client and a set of MAC addresses, generally the VLAN's gateway routers. Clients within the VLAN are not permitted to communicate among themselves directly. To communicate with another client, the client must use one of the specified gateway routers.

Syntax — `set security l2-restrict vlan vlan-id [mode {enable | disable}] [permit-mac mac-addr [mac-addr]]`

- *vlan-id* — VLAN name or number.
- **mode** — Enables or disables restriction of Layer 2 forwarding. {enable | disable}
- **permit-mac** *mac-addr* [*mac-addr*] — MAC addresses to which clients are allowed to forward data at Layer 2. You can specify up to four addresses.

Defaults — Layer 2 restriction is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 4.1.

Usage — You can specify multiple addresses by listing them on the same command line or by entering multiple commands. To change a MAC address, use the **clear security l2-restrict** command to remove it, then use the **set security l2-restrict** command to add the correct address.

Restriction of client traffic does not begin until you enable the permitted MAC list. Use the **mode enable** option with this command

Examples — The following command restricts Layer 2 forwarding of client data in VLAN *abc_air* to the gateway routers with MAC address *aa:bb:cc:dd:ee:ff* and *11:22:33:44:55:66*:

```
WX4400# set security l2-restrict vlan abc_air mode enable
permit-mac aa:bb:cc:dd:ee:ff 11:22:33:44:55:66
success: change accepted.
```

See Also

- **clear security l2-restrict** on page 105
- **clear security l2-restrict counters** on page 106
- **display security l2-restrict** on page 116

set vlan name

Creates a VLAN and assigns a number and name to it.

Syntax — `set vlan vlan-num name name`

- *vlan-num* — VLAN number. You can specify a number from 2 through 4093.
- *name* — String up to 16 alphabetic characters long.

Defaults — VLAN 1 is named *default* by default. No other VLANs have default names.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must assign a name to a VLAN (other than the default VLAN) before you can add ports to the VLAN.

3Com recommends that you do not use the name *default*. This name is already used for VLAN 1. 3Com also recommends that you do not rename the default VLAN.

You cannot use a number as the first character in a VLAN name. It is recommended that you do not use the same name with different capitalizations for VLANs. For example, do not configure two separate VLANs with the names *red* and *RED*.

VLAN names are case-sensitive for RADIUS authorization when a client roams to a wireless LAN switch. If the WX switch is not configured with the VLAN the client is on, but is configured with a VLAN that has the same spelling but different capitalization, authorization for the client fails. For example, if the client is on VLAN *red* but the WX switch to which the client roams has VLAN *RED* instead, RADIUS authorization fails.

Examples — The following command assigns the name *marigold* to VLAN 3:

```
WX4400# set vlan 3 name marigold
success: change accepted.
```

See Also

- **set vlan port** on page 125

set vlan port

Assigns one or more network ports to a VLAN. You also can add a virtual port to each network port by adding a tag value to the network port.

Syntax — `set vlan vlan-id port port-list [tag tag-value]`

- *vlan-id* — VLAN name or number.
- **port** *port-list* — List of physical ports.
- **tag** *tag-value* — Tag value that identifies a virtual port. You can specify a value from 1 through 4093.

By default, no ports are members of any VLANs. A wireless LAN switch cannot forward traffic on the network until you configure VLANs and add network ports to the VLANs.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You can combine this command with the **set port name** command to assign the name and add the ports at the same time.

If you do not specify a tag value, the WX switch sends untagged frames for the VLAN. If you do specify a tag value, the WX sends tagged frames only for the VLAN.

If you do specify a tag value, 3Com recommends that you use the same value as the VLAN number. MSS does not require the VLAN number and tag value to be the same but some other switches do.

Examples — The following command assigns the name *beige* to VLAN 11 and adds ports 1 through 3 to the VLAN:

```
WX1200# set vlan 11 name beige port 1-3
success: change accepted.
```

The following command adds port 6 to VLAN *beige* and assigns tag value 86 to the port:

```
WX1200# set vlan beige port 6 tag 86
success: change accepted.
```

See Also

- **clear security 12-restrict** on page 105
- **display vlan config** on page 118
- **set security l2-restrict** on page 123

**set vlan
tunnel-affinity**

Changes a wireless LAN switch's preferability within a mobility domain for tunneling user traffic for a VLAN. When a user roams to a WX switch that is not a member of the user's VLAN, the WX can forward the user traffic by tunneling to another WX switch that is a member of the VLAN.

Syntax — `set vlan vlan-id tunnel-affinity num`

- *vlan-id* — VLAN name or number.
- *num* — Preference of this switch for forwarding user traffic for the VLAN. You can specify a value from 1 through 10. A higher number indicates a greater preference.

Defaults — Each VLAN on a WX switch's network ports has an affinity value of 5 by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Increasing a WX switch's affinity value increases the WX's preferability for forwarding user traffic for the VLAN.

If more than one WX switch has the highest affinity value, MSS randomly selects one of the WX switches for the tunnel.

Examples — The following command changes the VLAN affinity for VLAN *beige* to 10:

```
WX4400# set vlan beige tunnel-affinity 10
success: change accepted.
```

See Also

- **display roaming vlan** on page 115
- **display vlan config** on page 118

set vlan profile

Configures entries in a VLAN profile that can be applied to an MAP for local switching.

Syntax — `set vlan-profile profile-name vlan vlan-name [tag tag-value]`

- *profile-name* — VLAN profile name.
- *vlan-name* — Name of a VLAN.
- *tag-value* — Optional tag value associated with the VLAN. When this value is set, it is used as the 802.1Q tag for the VLAN.

Defaults — If local switching is enabled on a MAP, but no VLAN profile is configured, then a default VLAN profile is used. The default VLAN profile includes a single VLAN named *default* that is not tagged.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — A VLAN profile consists of a list of VLANs and tags. When a VLAN profile is applied to a MAP, traffic for the VLANs specified in the VLAN profile is locally switched by the MAP instead of being tunneled back to an WX switch.

You enter a separate **set vlan-profile** command for each VLAN you want to add to the VLAN profile. A VLAN profile can contain up to 128 entries.

Examples — The following command adds an entry for VLAN *red* to VLAN profile *locals*:

```
WX# set vlan-profile locals vlan red
success: change accepted.
```

See Also

- **display fdb** on page 109
- **display vlan-profile** on page 120
- **clear vlan-profile** on page 108

6

QUALITY OF SERVICE COMMANDS

Use Quality of Service (QoS) commands to configure packet prioritization in MSS. Packet prioritization ensures that WX switches and MAP access points give preferential treatment to high-priority traffic such as voice and video.

(To override the prioritization for specific traffic, use access controls lists [ACLs] to set the Class of Service [CoS] for the packets. See “Security ACL Commands” on page 537.)

Commands by Usage

This chapter presents QoS commands alphabetically. Use Table 27 to locate commands in this chapter based on their use.

Table 27 QoS Commands by Usage

Type	Command
QoS Settings	display qos on page 133
	display qos dscp-table on page 134
	set qos cos-to-dscp-map on page 131
	set qos dscp-to-cos-map on page 132
	clear qos on page 129

clear qos

Resets the switch’s mapping of Differentiated Services Code Point (DSCP) values to internal QoS values.

The switch’s internal QoS map ensures that prioritized traffic remains prioritized while transiting through the WX switch. A WX switch uses the QoS map to do the following:

- Classify inbound packets by mapping their DSCP values to one of eight internal QoS values
- Classify outbound packets by marking their DSCP values based on the switch's internal QoS values

Syntax — `clear qos [cos-to-dscp-map [from-qos] | dscp-to-cos-map [from-dscp]]`

- **cos-to-dscp-map** — Resets the mapping between the specified internal QoS value and the DSCP values with which MSS marks outbound packets. QoS values are from 0 to 7.
- **dscp-to-cos-map** — Resets the mapping between the specified range of DSCP values and internal QoS value with which MSS classifies inbound packets.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.1.

Usage — To reset all mappings to their default values, use the **clear qos** command without the optional parameters.

Examples — The following command resets all QoS mappings:

```
WX1200# clear qos
success: change accepted.
```

The following command resets the mapping used to classify packets with DSCP value 44:

```
WX1200# clear qos dscp-to-qos-map 44
success: change accepted.
```

**set qos
cos-to-dscp-map**

Changes the value to which MSS maps an internal QoS value when marking outbound packets.

Syntax — `set qos cos-to-dscp-map level dscp dscp-value`

- *level* — Internal CoS value. You can specify a number from 0 to 7.
- **dscp** *dscp-value* — DSCP value. You can specify the value as a decimal number. Valid values are 0 to 63.

Defaults — The defaults are listed by the **display qos** command.

Access — Enabled.

History — Introduced in MSS Version 4.1.

Examples — The following command maps internal CoS value 5 to DSCP value 50:

```
WX1200# set qos cos-to-dscp-map 5 dscp 50
warning: cos 5 is marked with dscp 50 which will be
classified as cos 6
```

If the change results in a change to CoS, MSS displays a warning message indicating the change. In this example, packets that receive CoS 5 upon ingress will be marked with a DSCP value equivalent to CoS 6 upon egress.

See Also

- **set qos dscp-to-cos-map** on page 132
- **display qos** on page 133

**set qos
dscp-to-cos-map**

Changes the internal QoS value to which MSS maps a packet's DSCP value when classifying inbound packets.

Syntax — `set qos dscp-to-cos-map dscp-range cos level`

- *dscp-range* — You can specify the values as decimal numbers. Valid decimal values are 0 to 63. To specify a range, use the following format: 40-56. Specify the lower number first.
- *cos level* — Internal QoS value. You can specify a number from 0 to 7.

Defaults — The defaults are listed by the **display qos** command.

Access — Enabled.

History — Introduced in MSS Version 4.1.

Examples — The following command maps DSCP values 40-56 to internal CoS value 6:

```
WX1200# set qos dscp-to-cos-map 40-56 cos 6
warning: cos 5 is marked with dscp 63 which will be
classified as cos 7
warning: cos 7 is marked with dscp 56 which will be
classified as cos 6
```

As shown in this example, if the change results in a change to CoS, MSS displays a warning message indicating the change.

See Also

- **set qos cos-to-dscp-map** on page 131
- **display qos** on page 133

display qos

Displays the switch's QoS settings.

Syntax — `display qos [default]`

- `default` — Displays the default mappings.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.1.

Examples — The following command displays the default QoS settings:

```
WX1200# display qos default
```

```
Ingress QoS Classification Map (dscp-to-cos)
```

Ingress DSCP	CoS Level									
	0	1	2	3	4	5	6	7	8	9
00-09	0	0	0	0	0	0	0	0	0	1
10-19	1	1	1	1	1	1	1	2	2	2
20-29	2	2	2	2	3	3	3	3	3	3
30-39	3	3	4	4	4	4	4	4	4	4
40-49	5	5	5	5	5	5	5	5	5	6
50-59	6	6	6	6	6	6	6	7	7	7
60-63	7	7	7	7						

```
Egress QoS Marking Map (cos-to-dscp)
```

CoS Level	0	1	2	3	4	5
6						
7						
Egress DSCP	0	8	16	24	32	40
48						
56						
Egress ToS byte	0x00	0x20	0x40	0x60	0x80	0xA0
0xC0						
0xE0						

See Also

- `display qos dscp-table` on page 134

**display qos
dscp-table**

Displays a table that maps Differentiated Services Code Point (DSCP) values to their equivalent combinations of IP precedence values and IP ToS values.

Syntax — `display qos dscp-table`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0 as the **display security acl dscp** command and renamed in MSS Version 4.1.

Examples — The following command displays the table:

```
WX1200# display qos dscp-table
```

DSCP		TOS		precedence	tos
dec	hex	dec	hex		
0	0x00	0	0x00	0	0
1	0x01	4	0x04	0	2
2	0x02	8	0x08	0	4
...					
63	0x3f	252	0xfc	7	14

See Also

- **display qos** on page 133

7

IP SERVICES COMMANDS

Use IP services commands to configure and manage IP interfaces, management services, the Domain Name Service (DNS), Network Time Protocol (NTP), aliases, and to ping a host or trace a route.

Commands by Usage

This chapter presents IP services commands alphabetically. Use Table 28 to locate the commands in this chapter based on their use.

Table 28 IP Services Commands by Usage

Type	Command
IP Interface	set interface on page 170
	set interface dhcp-client on page 171
	set interface status on page 173
	display interface on page 152
	display dhcp-client on page 148
System IP Address	clear interface on page 137
	set system ip-address on page 203
	clear system ip-address on page 146
IP Route	set ip route on page 178
	display ip route on page 156
	clear ip route on page 140
SSH Management	set ip ssh server on page 181
	set ip ssh on page 180
Telnet Management	set ip telnet on page 181
	set ip telnet server on page 182
	display ip telnet on page 158
	clear ip telnet on page 141

Table 28 IP Services Commands by Usage (continued)

Type	Command
HTTPS Management	set ip https server on page 177
	display ip https on page 155
DNS	set ip dns on page 175
	set ip dns domain on page 175
	set ip dns server on page 176
	display ip dns on page 154
	clear ip dns domain on page 139
	clear ip dns server on page 139
IP Alias	set ip alias on page 174
	display ip alias on page 153
	clear ip alias on page 138
Time and Date	set timedate on page 204
	set timezone on page 205
	set summertime on page 202
	display timedate on page 165
	display timezone on page 165
	display summertime on page 164
	clear timezone on page 146
clear summertime on page 145	
NTP	set ntp on page 183
	set ntp server on page 184
	set ntp update-interval on page 185
	display ntp on page 159
	clear ntp server on page 141
	clear ntp update-interval on page 142
ARP	set arp on page 168
	set arp agingtime on page 169
	display dhcp-client on page 148
SNMP	set snmp protocol on page 197
	set snmp security on page 198
	set snmp community on page 185
	set snmp usm on page 199

Table 28 IP Services Commands by Usage (continued)

Type	Command
	set snmp notify profile on page 187
	set snmp notify target on page 192
	set ip snmp server on page 180
	display snmp status on page 163
	display snmp community on page 161
	display snmp usm on page 164
	display snmp notify profile on page 162
	display snmp notify target on page 162
	display snmp counters on page 162
	clear snmp community on page 143
	clear snmp usm on page 144
	clear snmp notify profile on page 143
	clear snmp notify target on page 144
Ping	ping on page 166
Telnet Client	telnet on page 206
Traceroute	traceroute on page 207
DHCP server	set interface dhcp-server on page 172
	display dhcp-server on page 150

clear interface

Removes an IP interface.

Syntax — `clear interface vlan-id ip`

- *vlan-id* — VLAN name or number

Defaults — None.**Access** — Enabled.**History** — Introduced in MSS Version 3.0.**Usage** — If the interface you want to remove is configured as the system IP address, removing the address can interfere with system tasks using the system IP address, including the following:

- Mobility domain operations

- Topology reporting for dual-homed MAP access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Examples — The following command removes the IP interface configured on VLAN *mauve*:

```
WX1200# clear interface mauve ip
success: cleared ip on vlan mauve
```

See Also

- **set interface** on page 170
- **set interface dhcp-client** on page 171
- **display interface** on page 152

clear ip alias

Removes an alias, which is a string that represents an IP address.

Syntax — `clear ip alias name`

name — Alias name

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes the alias `server1`:

```
WX1200# clear ip alias server1
success: change accepted.
```

See Also

- **display ip alias** on page 153

clear ip dns domain Removes the default DNS domain name.

Syntax — `clear ip dns domain`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes the default DNS domain name from a WX switch:

```
WX1200# clear ip dns domain
Default DNS domain name cleared.
```

See Also

- **clear ip dns server** on page 139
- **display ip dns** on page 154
- **set ip dns** on page 175
- **set ip dns domain** on page 175
- **set ip dns server** on page 176

clear ip dns server Removes a DNS server from a WX switch configuration.

Syntax — `clear ip dns server ip-addr`

- *ip-addr* — IP address of a DNS server.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes DNS server 10.10.10.69 from a WX configuration:

```
WX4400# clear ip dns server 10.10.10.69
success: change accepted.
```

See Also

- **clear ip dns domain** on page 139
- **display ip dns** on page 154
- **set ip dns** on page 175
- **set ip dns domain** on page 175
- **set ip dns server** on page 176

clear ip route

Removes a route from the IP route table.

Syntax — `clear ip route {default | ip-addr mask | ip-addr/mask-length} default-router`

- *default* — Default route.



default is an alias for IP address 0.0.0.0/0.

- *ip-addr mask* — IP address and subnet mask for the route destination, in dotted decimal notation (for example, 10.10.10.10 255.255.255.0).
- *ip-addr/mask-length* — IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24).
- *default-router* — IP address, DNS hostname, or alias of the next-hop router.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes the route to destination 10.10.10.68/24 through router 10.10.10.1:

```
WX1200# clear ip route 10.10.10.68/24 10.10.10.1
success: change accepted.
```

See Also

- **display ip route** on page 156
- **set ip route** on page 178

clear ip telnet

Resets the Telnet server TCP port number to its default value. A WX listens for Telnet management traffic on the Telnet server port.

Syntax — `clear ip telnet`

Defaults — The default Telnet port number is 23.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command resets the TCP port number for Telnet management traffic to its default:

```
WX4400# clear ip telnet
success: change accepted.
```

See Also

- **display ip https** on page 155
- **display ip telnet** on page 158
- **set ip https server** on page 177
- **set ip telnet** on page 181
- **set ip telnet server** on page 182

clear ntp server

Removes an NTP server from a WX configuration.

Syntax — `clear ntp server {ip-addr | all}`

- *ip-addr* — IP address of the server to remove, in dotted decimal notation.
- **all** — Removes all NTP servers from the configuration.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes NTP server 192.168.40.240 from a WX switch configuration:

```
WX4400# clear ntp server 192.168.40.240
success: change accepted.
```

See Also

- **clear ntp update-interval** on page 142
- **display ntp** on page 159
- **set ntp** on page 183
- **set ntp server** on page 184
- **set ntp update-interval** on page 185

clear ntp update-interval

Resets the NTP update interval to the default value.

Syntax — `clear ntp update-interval`

Defaults — The default NTP update interval is 64 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To reset the NTP interval to the default value, type the following command:

```
WX4400# clear ntp update-interval
success: change accepted.
```

See Also

- **clear ntp server** on page 141
- **display ntp** on page 159
- **set ntp** on page 183
- **set ntp server** on page 184
- **set ntp update-interval** on page 185

clear snmp community

Clears an SNMP community string.

Syntax — `clear snmp community name comm-string`

- *comm-string* — Name of the SNMP community you want to clear.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command clears community string *setswitch2*:

```
WX1200# clear snmp community name setswitch2
success: change accepted.
```

See Also

- **set snmp community** on page 185
- **display snmp community** on page 161

clear snmp notify profile

Clears an SNMP notification profile.

Syntax — `clear snmp notify profile profile-name`

- *profile-name* — Name of the notification profile you are clearing.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command clears notification profile *snmpprof_rfdetect*:

```
WX1200# clear snmp notify profile snmpprof_rfdetect
success: change accepted.
```

See Also

- **set snmp notify profile** on page 187
- **display snmp notify profile** on page 162

clear snmp notify target

Clears an SNMP notification target.

Syntax — `clear snmp notify target target-num`

- *target-num* — ID of the target.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command clears notification target 3:

```
WX1200# clear snmp notify target 3
success: change accepted.
```

See Also

- **set snmp notify target** on page 192
- **display snmp notify target** on page 162

clear snmp usm

Clears an SNMPv3 user.

Syntax — `clear snmp usm usm-username`

- *usm-username* — Name of the SNMPv3 user you want to clear.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command clears SNMPv3 user *snmpmgr1*:

```
WX1200# clear snmp usm snmpmgr1
success: change accepted.
```

See Also

- **set snmp usm** on page 199
- **display snmp usm** on page 164

clear summertime

Clears the summertime setting from a WX.

Syntax — `clear summertime`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To clear the summertime setting from a WX, type the following command:

```
WX1200# clear summertime
success: change accepted.
```

See Also

- **clear timezone** on page 146
- **display summertime** on page 164
- **display timedate** on page 165
- **display timezone** on page 165
- **set summertime** on page 202
- **set timedate** on page 204
- **set timezone** on page 205

clear system ip-address

Clears the system IP address.

CAUTION: *Clearing the system IP address disrupts the system tasks that use the address.*

Syntax — `clear system ip-address`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Clearing the system IP address can interfere with system tasks that use the system IP address, including the following:

- Mobility Domain operations
- Topology reporting for dual-homed MAP access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Examples — To clear the system IP address, type the following command:

```
WX1200# clear system ip-address
success: change accepted.
```

See Also

- **display system** on page 47
- **set system ip-address** on page 203

clear timezone

Clears the time offset for the WX real-time clock from Coordinated Universal Time (UTC). UTC is also known as Greenwich Mean Time (GMT).

Syntax — `clear timezone`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To return the WX real-time clock to UTC, type the following command:

```
WX4400# clear timezone
success: change accepted.
```

See Also

- **clear summertime** on page 145
- **set summertime** on page 202
- **set timedate** on page 204
- **set timezone** on page 205
- **display summertime** on page 164
- **display timedate** on page 165
- **display timezone** on page 165

display arp

Shows the ARP table.

Syntax — `display arp [ip-addr]`

- *ip-addr* — IP address.

Defaults — If you do not specify an IP address, the entire ARP table is displayed.

Usage — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays ARP entries:

```
WX4400# display arp
ARP aging time: 1200 seconds
```

Host	HW Address	VLAN	Type	State
10.5.4.51	00:0b:0e:02:76:f5	1	DYNAMIC	RESOLVED
10.5.4.53	00:0b:0e:02:76:f7	1	LOCAL	RESOLVED

Table 29 describes the fields in this display.

Table 29 Output for display arp

Field	Description
ARP aging time	Number of seconds a dynamic entry can remain unused before MSS removes the entry from the ARP table.
Host	IP address, hostname, or alias.
HW Address	MAC address mapped to the IP address, hostname, or alias.
VLAN	VLAN the entry is for.
Type	Entry type: <ul style="list-style-type: none"> ▪ DYNAMIC — Entry was learned from network traffic and ages out if unused for longer than the ARP aging timeout. ▪ LOCAL — Entry for the WX switch's MAC address. Each VLAN has one local entry for the WX switch's MAC address. ▪ PERMANENT — Entry does not age out and remains in the configuration even following a reboot. ▪ STATIC — Entry does not age out but is removed after a reboot.
State	Entry state: <ul style="list-style-type: none"> ▪ RESOLVING — MSS sent an ARP request for the entry and is waiting for the reply. ▪ RESOLVED — Entry is resolved.

See Also

- **set arp** on page 168
- **set arp agingtime** on page 169

display dhcp-client Displays DHCP client information for all VLANs.

Syntax — `display dhcp-client`

Defaults — None.

Access — All.

History — Introduced in MSS Version 4.0.

Examples — The following command displays DHCP client information:

```
WX1200# display dhcp-client
Interface:                corpvlan(4)
Configuration Status:    Enabled
DHCP State:              IF_UP
Lease Allocation:        65535 seconds
Lease Remaining:        65532 seconds
IP Address:              10.3.1.110
Subnet Mask:             255.255.255.0
Default Gateway:         10.3.1.1
DHCP Server:            10.3.1.4
DNS Servers:             10.3.1.29
DNS Domain Name:        mycorp.com
```

Table 30 describes the fields in this display.

Table 30 Output for display dhcp-client

Field	Description
Interface	VLAN name and number.
Configuration Status	Status of the DHCP client on this VLAN: <ul style="list-style-type: none"> ■ Enabled ■ Disabled
DHCP State	State of the IP interface: <ul style="list-style-type: none"> ■ IF_UP ■ IF_DOWN
Lease Allocation	Duration of the address lease.
Lease Remaining	Number of seconds remaining before the address lease expires.
IP Address	IP address received from the DHCP server
Subnet Mask	Network mask of the IP address received from the DHCP server.
Default Gateway	Default gateway IP address received from the DHCP server. If the address is 0.0.0.0, the server did not provide an address.
DHCP Server	IP address of the DHCP server.
DNS Servers	DNS server IP address(es) received from the DHCP server.
DNS Domain Name	Default DNS domain name received from the DHCP server.

See Also

- **set interface dhcp-client** on page 171

display dhcp-server Displays MSS DHCP server information.

Syntax — **display dhcp-server** [**interface** *vlan-id*] [**verbose**]

- **interface** *vlan-id* — Displays the IP addresses leased by the specified VLAN.
- **verbose** — Displays configuration and status information for the MSS DHCP server.

Defaults — None.

Access — All.

History — Introduced in MSS Version 4.0.

Examples — The following command displays the addresses leased by the MSS DHCP server:

```
WX1200# display dhcp-server
VLAN Name      Address          MAC                Lease Remaining (sec)
-----
1 default      10.10.20.2      00:01:02:03:04:05 12345
1 default      10.10.20.3      00:01:03:04:06:07 2103
2 red-vlan     192.168.1.5     00:01:03:04:06:08 102
2 red-vlan     192.168.1.7     00:01:03:04:06:09 16789
```

The following command displays configuration and status information for each VLAN on which the DHCP server is configured:

```
WX1200# display dhcp-server verbose
Interface:      0 (Direct AP)
Status:         UP
Address Range:  10.0.0.1-10.0.0.253

Interface:      default(1)
Status:         UP
Address Range:  10.10.20.2-10.10.20.254
DHCP Clients:
  Hardware Address: 00:01:02:03:04:05
  State:           BOUND
  Lease Allocation: 43200 seconds
  Lease Remaining: 12345 seconds
  IP Address:      10.10.20.2
  Subnet Mask:     255.255.255.0
```

```

Default Gateway:      10.10.20.1
DNS Servers:         10.10.20.4 10.10.20.5
DNS Domain Name:    mycorp.com

```

Table 31 and Table 32 describe the fields in these displays.

Table 31 Output for display dhcp-server

Field	Description
VLAN	VLAN number
Name	VLAN name
Address	IP address leased by the server.
MAC Address	MAC address of the device that holds the least for the address.
Lease Remaining	Number of seconds remaining before the address lease expires.

Table 32 Output for display dhcp-server verbose

Field	Description
Interface	VLAN name and number.
Status	Status of the interface: <ul style="list-style-type: none"> ▪ UP ▪ DOWN
Address Range	Range from which the server can lease addresses.
Hardware Address	MAC address of the DHCP client.
Lease Remaining	Number of seconds remaining before the address lease expires.
State	State of the address lease: <ul style="list-style-type: none"> ▪ SUSPEND—MSS is checking for the presence of another DHCP server on the subnet. This is the initial state of the MSS DHCP server. The MSS DHCP server remains in this state if another DHCP server is detected. ▪ CHECKING—MSS is using ARP to verify whether the address is available. ▪ OFFERING—MSS offered the address to the client and is waiting for the client to send a DHCPREQUEST for the address. ▪ BOUND—The client accepted the address. ▪ HOLDING—The address is already in use and is therefore unavailable.
Lease Allocation	Duration of the address lease, in seconds.
Lease Remaining	Number of seconds remaining before the address lease expires.

Table 32 Output for display dhcp-server verbose

Field	Description
IP Address	IP address leased to the client.
Subnet Mask	Network mask of the IP address leased to the client.
Default Gateway	Default gateway IP address included in the DHCP Offer to the client.
DNS Server	DNS server IP address(es) included in the DHCP Offer to the client.
DNS Domain Name	Default DNS domain name included in the DHCP Offer to the client.

See Also

- **set interface dhcp-server** on page 172

display interface

Displays the IP interfaces configured on the WX.

Syntax — **display interface** [*vlan-id*]

- *vlan-id* — VLAN name or number.

Defaults — If you do not specify a VLAN ID, interfaces for all VLANs are displayed.

Usage — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays all the IP interfaces configured on a WX switch:

```
WX4400# display interface
VLAN Name          Address           Mask              Enabled State   RIB
-----
  1 default         10.10.10.10      255.255.255.0    YES      Up      ipv4
  2 mauve          10.10.20.10      255.255.255.0    NO       Down    ipv4
4094 web-aaa       10.10.10.1       255.255.255.0    YES      Up      ipv4
```

Table 33 describes the fields in this display.

Table 33 Output for display interface

Field	Description
VLAN	VLAN number
Name	VLAN name
Address	IP address
Mask	Subnet mask
Enabled	Administrative state: <ul style="list-style-type: none"> ▪ YES (enabled) ▪ NO (disabled)
State	Link state: <ul style="list-style-type: none"> ▪ Up (operational) ▪ Down (unavailable)
RIB	Routing Information Base

See Also

- **clear interface** on page 137
- **set interface** on page 170
- **set interface dhcp-client** on page 171

display ip alias

Displays the IP aliases configured on the WX.

Syntax — `display ip alias [name]`

- *name* — Alias string.

Defaults — If you do not specify an alias name, all aliases are displayed.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command displays all the aliases configured on a WX switch:

```
WX4400# display ip alias
Name                               IP Address
-----
HR1                                 192.168.1.2
payroll                             192.168.1.3
radius1                             192.168.7.2
```

Table 34 describes the fields in this display.

Table 34 Output for display ip alias

Field	Description
Name	Alias string.
IP Address	IP address associated with the alias.

See Also

- **clear ip alias** on page 138
- **set ip alias** on page 174

display ip dns

Displays the DNS servers used by the WX.

Syntax — `display ip dns`

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays the DNS information:

```
WX4400# display ip dns
Domain Name: example.com
DNS Status: enabled
IP Address                               Type
-----
10.1.1.1                                 PRIMARY
10.1.1.2                                 SECONDARY
10.1.2.1                                 SECONDARY
```

Table 35 describes the fields in this display.

Table 35 Output for display ip dns

Field	Description
Domain Name	Default domain name configured on the WX switch

Table 35 Output for display ip dns (continued)

Field	Description
DNS Status	Status of the WX switch's DNS client: <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled
IP Address	IP address of the DNS server
Type	Server type: <ul style="list-style-type: none"> ▪ PRIMARY ▪ SECONDARY

See Also

- **clear ip dns domain** on page 139
- **clear ip dns server** on page 139
- **set ip dns** on page 175
- **set ip dns domain** on page 175
- **set ip dns server** on page 176

display ip https

Shows information about the HTTPS management port.

Syntax — `display ip https`

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command shows the status and port number for the HTTPS management interface to the WX switch:

```
WX4400# display ip https
HTTPS is enabled
HTTPS is set to use port 443
```

Last 10 Connections:

IP Address	Last Connected	Time Ago (s)
10.10.10.56	2003/05/09 15:51:26 pst	349

Table 36 describes the fields in this display.

Table 36 Output for display ip https

Field	Description
HTTPS is enabled/disabled	State of the HTTPS server: <ul style="list-style-type: none"> ■ Enabled ■ Disabled
HTTPS is set to use port	TCP port number on which the WX switch listens for HTTPS connections.
Last 10 connections	List of the last 10 devices to establish connections to the WX HTTPS server.
IP Address	IP address of the device that established the connection. Note: If a browser connects to a WX from behind a proxy, then only the proxy IP address is shown. If multiple browsers connect using the same proxy, the proxy address appears only once in the output.
Last Connected	Time when the WX switch established the HTTPS connection to the WX switch.
Time Ago (s)	Number of seconds since the device established the HTTPS connection to the WX switch.

See Also

- **clear ip telnet** on page 141
- **display ip telnet** on page 158
- **set ip https server** on page 177
- **set ip telnet** on page 181
- **set ip telnet server** on page 182

display ip route

Displays the IP route table on the WX.

Syntax — **display ip route** [*destination*]

- *destination* — Route destination IP address, in dotted decimal notation.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Usage — When you add an IP interface to a VLAN that is up, MSS adds direct and local routes for the interface to the route table. If the VLAN is down, MSS does not add the routes. If you add an interface to a VLAN but the routes for that interface do not appear in the route table, use the **display vlan config** command to check the VLAN state.

If you add a static route and the route's state is shown as Down, use the **display interface** command to verify that the route has an IP interface in the gateway router's subnet. MSS cannot resolve a static route unless one of the WX switch's VLANs has an interface in the gateway router's subnet. If the WX switch has such an interface but the static route is still down, use the **display vlan config** command to check the state of the VLAN's ports.

Examples — The following command shows all routes in a WX IP route table:

```
WX4400# display ip route
Router table for IPv4
Destination/Mask  Proto  Metric  NH-Type  Gateway  VLAN:Interface
-----
0.0.0.0/ 0  Static  1 Router  10.0.1.17  Down
0.0.0.0/ 0  Static  2 Router  10.0.2.17  vlan:2:ip
10.0.2.1/24 IP      0 Direct
10.0.2.1/32 IP      0 Direct  vlan:2:ip
10.0.2.255/32 IP     0 Direct  vlan:2:ip:10.0.1.1/24
224.0.0.0/ 4  IP      0 Local   MULTICAST
```

Table 37 describes the fields in this display.

Table 37 Output of display ip route

Field	Description
Destination/Mask	IP address and subnet mask of the route destination. The 244.0.0.0 route is automatically added by MSS and supports the IGMP snooping feature.
Proto	Protocol that added the route to the IP route table. The protocol can be one of the following: <ul style="list-style-type: none"> ■ IP — MSS added the route. ■ Static — An administrator added the route.
Metric	Cost for using the route.

Table 37 Output of display ip route (continued)

Field	Description
NH-Type	<p>Next-hop type:</p> <ul style="list-style-type: none"> ▪ Local — Route is for a local interface. MSS adds the route when you configure an IP address on the WX. ▪ Direct — Route is for a locally attached subnet. MSS adds the route when you add an interface in the same subnet to the WX. ▪ Router — Route is for a remote destination. A WX switch forwards traffic for the destination to the gateway router.
Gateway	<p>Next-hop router for reaching the route destination.</p> <p>This field applies only to static routes.</p>
VLAN:Interface	<p>Destination VLAN, protocol type, and IP address of the route. Because direct routes are for local interfaces, a destination IP address is not listed.</p> <p>The destination for the IP multicast route is MULTICAST.</p> <p>For static routes, the value Down means the WX does not have an interface to the destination next-hop router. To provide an interface, configure an IP interface that is in the same IP subnet as the next-hop router. The IP interface must be on a VLAN with the port attached to the default router.</p>

See Also

- **clear ip route** on page 140
- **display interface** on page 152
- **display vlan config** on page 118
- **set interface** on page 170
- **set ip route** on page 178

display ip telnet

Shows information about the Telnet management port.

Syntax — `display ip telnet`

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command shows the status and port number for the Telnet management interface to the WX switch:

```
WX4400> display ip telnet
```

```
Server Status          Port
-----
Enabled                23
```

Table 38 describes the fields in this display.

Table 38 Output for display ip telnet

Field	Description
Server Status	State of the HTTPS server: <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled
Port	TCP port number on which the WX switch listens for Telnet management traffic.

See Also

- **clear ip telnet** on page 141
- **display ip https** on page 155
- **set ip https server** on page 177
- **set ip telnet** on page 181
- **set ip telnet server** on page 182

display ntp

Shows NTP client information.

Syntax — `display ntp`

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — To display NTP information for a WX switch, type the following command:

```
WX4400> display ntp
NTP client: enabled
Current update-interval: 20(secs)
Current time: Fri Feb 06 2004, 12:02:57
Timezone is set to 'PST', offset from UTC is -8:0 hours.
Summertime is enabled.
Last NTP update: Fri Feb 06 2004, 12:02:46
NTP Server          Peer state          Local State
-----
192.168.1.5        SYSPEER             SYNCED
```

Table 39 describes the fields in this display.

Table 39 Output for display ntp

Field	Description
NTP client	State of the NTP client. The state can be one of the following: <ul style="list-style-type: none"> ■ Enabled ■ Disabled
Current update-interval	Number of seconds between queries sent by the WX to the NTP servers for updates.
Current time	System time that was current on the WX when you pressed Enter after typing the display ntp command.
Timezone	Time zone configured on the WX switch. MSS offsets the time reported by the NTP server based on the time zone. This field is displayed only if you change the time zone.
Summertime	Summertime period configured on the WX switch. MSS offsets the system time +1 hour and returns it to standard time for daylight savings time or a similar summertime period that you set. This field is displayed only if you enable summertime.
Last NTP update	Time when the WX received the most recent update from an NTP server.
NTP Server	IP address of the NTP server.

Table 39 Output for display ntp (continued)

Field	Description
Peer state	State of the NTP session from the point of view of the NTP server: <ul style="list-style-type: none"> ▪ CORRECT ▪ REJECT ▪ SELCAND ▪ SYNCCAND ▪ SYSPEER
Local state	State of the NTP session from the point of view of the WX NTP client: <ul style="list-style-type: none"> ▪ INITED ▪ START ▪ SYNCED

See Also

- **clear ntp server** on page 141
- **clear summertime** on page 145
- **clear timezone** on page 146
- **display timezone** on page 165
- **set ntp** on page 183
- **set ntp server** on page 184
- **set summertime** on page 202
- **set timezone** on page 205

display snmp community

Displays the configured SNMP community strings.

Syntax — `display snmp community`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

See Also

- **clear snmp community** on page 143
- **set snmp community** on page 185

display snmp counters

Displays SNMP statistics counters.

Syntax — `display snmp counters`

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

display snmp notify profile

Displays SNMP notification profiles.

Syntax — `display snmp notify profile`

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

See Also

- **clear snmp notify profile** on page 143
- **set snmp notify profile** on page 187

display snmp notify target

Displays SNMP notification targets.

Syntax — `display snmp notify target`

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

See Also

- **clear snmp notify target** on page 144
- **set snmp notify target** on page 192

display snmp status Displays SNMP version and status information.

Syntax — `display snmp status`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

See Also

- **set snmp community** on page 185
- **set snmp notify target** on page 192
- **set snmp notify profile** on page 187
- **set snmp protocol** on page 197
- **set snmp security** on page 198
- **set snmp usm** on page 199
- **display snmp community** on page 161
- **display snmp counters** on page 162
- **display snmp notify profile** on page 162
- **display snmp notify target** on page 162
- **display snmp usm** on page 164

display snmp usm Displays information about SNMPv3 users.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.0.

See Also

- **clear snmp usm** on page 144
- **display snmp usm** on page 164

display summertime Displays a WX offset time from its real-time clock time.

Syntax — `display summertime`

Defaults — There is no summertime offset by default.

Access — All.

History —Introduced in MSS Version 3.0.

Examples — To display the summertime setting on a WX, type the following command:

```
WX1200# display summertime
Summertime is enabled, and set to 'PDT'.
Start   : Sun Apr 04 2004, 02:00:00
End     : Sun Oct 31 2004, 02:00:00
Offset  : 60 minutes
Recurring : yes, starting at 2:00 am of first Sunday of April
           and ending at 2:00 am on last Sunday of October.
```

See Also

- **clear summertime** on page 145
- **clear timezone** on page 146
- **display timedate** on page 165
- **display timezone** on page 165
- **set summertime** on page 202

- **set timedate** on page 204
- **set timezone** on page 205

display timedate

Shows the date and time of day currently set on a WX real-time clock.

Syntax — `display timedate`

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — To display the time and date set on a WX real-time clock, type the following command:

```
WX1200# display timedate
Sun Feb 29 2004, 23:59:02 PST
```

See Also

- **clear summertime** on page 145
- **clear timezone** on page 146
- **display summertime** on page 164
- **display timezone** on page 165
- **set summertime** on page 202
- **set timedate** on page 204
- **set timezone** on page 205

display timezone

Displays the time offset for the real-time clock from UTC on a WX.

Syntax — `display timezone`

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — To display the offset from UTC, type the following command:

```
WX4400# display timezone
Timezone set to 'pst', offset from UTC is -8 hours
```

See Also

- **clear summertime** on page 145
- **clear timezone** on page 146
- **display summertime** on page 164
- **display timedate** on page 165
- **set summertime** on page 202
- **set timedate** on page 204
- **set timezone** on page 205

ping

Tests IP connectivity between a WX and another device. MSS sends an Internet Control Message Protocol (ICMP) echo packet to the specified device and listens for a reply packet.

Syntax — `ping host [count num-packets] [dnf] [flood] [interval time] [size size] [source-ip ip-addr | vlan-name]`

- *host* — IP address, MAC address, hostname, alias, or user to ping.
- **count num-packets** — Number of ping packets to send. You can specify from 0 through 2,147,483,647. If you enter 0, MSS pings continuously until you interrupt the command.
- **dnf** — Enables the Do Not Fragment bit in the ping packet to prevent fragmenting the packet.
- **flood** — Sends new ping packets as quickly as replies are received, or 100 times per second, whichever is greater.



Use the flood option sparingly. This option creates a lot of traffic and can affect other traffic on the network.

- **interval time** — Time interval between ping packets, in milliseconds. You can specify from 100 through 10,000.
- **size size** — Packet size, in bytes. You can specify from 56 through 65,507.



Because the WX switch adds header information, the ICMP packet size is 8 bytes larger than the size you specify.

- **source-ip** *ip-addr* — IP address, in dotted decimal notation, to use as the source IP address in the ping packets.
- **source-ip** *vlan-name* — VLAN name to use as the ping source. MSS uses the IP address configured on the VLAN as the source IP address in the ping packets.

Defaults

- **count** — 5.
- **dnf** — Disabled.
- **interval** — 100 (one tenth of a second)
- **size** — 56.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To stop a ping command that is in progress, press Ctrl+C.

Examples — The following command pings a WX switch that has IP address 10.1.1.1:

```
WX1200# ping 10.1.1.1
PING 10.1.1.1 (10.1.1.1) from 10.9.4.34 : 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=0.769 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=0.628 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=0.676 ms
64 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=0.619 ms
64 bytes from 10.1.1.1: icmp_seq=5 ttl=255 time=0.608 ms
--- 10.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0 errors, 0% packet loss
```

See Also

- **traceroute** on page 207

set arp

Adds an ARP entry to the ARP table.

Syntax — `set arp {permanent | static | dynamic }
ip-addr mac-addr`

- **permanent** — Adds a permanent entry. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
- **static** — Adds a static entry. A static entry does not age out, but the entry does not remain in the database after a reboot, reset, or power cycle.
- **dynamic** — Adds a dynamic entry. A dynamic entry is automatically removed if the entry ages out, or after a reboot, reset, or power cycle.
- *ip-addr* — IP address of the entry, in dotted decimal notation.
- *mac-addr* — MAC address to map to the IP address. Use colons to separate the octets (for example, 00:11:22:aa:bb:cc).

Defaults — The default aging timeout is 1200 seconds.

Access — Enabled.

History— Introduced in MSS Version 3.0.

Examples — The following command adds a static ARP entry that maps IP address 10.10.10.1 to MAC address 00:bb:cc:dd:ee:ff:

```
WX1200# set arp static 10.10.10.1 00:bb:cc:dd:ee:ff  
success: added arp 10.10.10.1 at 00:bb:cc:dd:ee:ff on VLAN 1
```

See Also

- **set arp agingtime** on page 169
- **telnet** on page 206

set arp agingtime Changes the aging timeout for dynamic ARP entries.

Syntax — `set arp agingtime seconds`

- *seconds* — Number of seconds an entry can remain unused before MSS removes the entry. You can specify from 0 through 1,000,000. To disable aging, specify 0.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Aging applies only to dynamic entries.

To reset the ARP aging timeout to its default value, use the **set arp agingtime 1200** command.

Examples — The following command changes the ARP aging timeout to 1800 seconds:

```
WX1200# set arp agingtime 1800
success: set arp aging time to 1800 seconds
```

The following command disables ARP aging:

```
WX1200# set arp agingtime 0
success: set arp aging time to 0 seconds
```

See Also

- **set arp** on page 168
- **telnet** on page 206

set interface

Configures an IP interface on a VLAN.

Syntax — **set interface** *vlan-id* **ip**
{*ip-addr mask* | *ip-addr/mask-length*}

- *vlan-id* — VLAN name or number.
- *ip-addr mask* — IP address and subnet mask in dotted decimal notation (for example, 10.10.10.10 255.255.255.0).
- *ip-addr/mask-length* — IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24).

Defaults — None.

Access — Enabled.

History— Introduced in MSS Version 3.0.

Usage — You can assign one IP interface to each VLAN.

If an interface is already configured on the specified VLAN, this command replaces the interface. If you replace an interface in use as the system IP address, replacing the interface can interfere with system tasks that use the system IP address, including the following:

- Mobility domain operations
- Topology reporting for dual-homed MAP access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Examples — The following command configures IP interface 10.10.10.10/24 on VLAN default:

```
WX1200# set interface default ip 10.10.10.10/24  
success: set ip address 10.10.10.10 netmask 255.255.255.0 on vlan default
```

The following command configures IP interface 10.10.20.10 255.255.255.0 on VLAN mauve:

```
WX1200# set interface mauve ip 10.10.20.10 255.255.255.0  
success: set ip address 10.10.20.10 netmask 255.255.255.0 on vlan mauve
```

See Also

- **clear interface** on page 137
- **display interface** on page 152
- **set interface dhcp-client** on page 171

set interface dhcp-client

Configures the DHCP client on a VLAN and allows the VLAN to obtain its IP interface from a DHCP server.

Syntax — `set interface vlan-id ip dhcp-client {enable | disable}`

- `vlan-id` — VLAN name or number.
- `enable` — Enables the DHCP client on the VLAN.
- `disable` — Disables the DHCP client on the VLAN.

Defaults — The DHCP client is enabled by default on an unconfigured WXR100 when the factory reset switch is pressed and held during power on.

The DHCP client is disabled by default on all other WX models, and is disabled on a WXR100 if it is already configured or the factory reset switch is not pressed and held during power on.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — You can enable the DHCP client on one VLAN only. You can configure the DHCP client on more than one VLAN, but the client can be active on only one VLAN.

MSS also has a configurable DHCP server. (See **set interface dhcp-server** on page 172.) You can configure a DHCP client and DHCP server on the same VLAN, but only the client or the server can be enabled. The DHCP client and DHCP server cannot both be enabled on the same VLAN at the same time.

Examples — The following command enables the DHCP client on VLAN *corpvlan*:

```
WX1200# set interface corpvlan ip dhcp-client enable
success: change accepted.
```

See Also

- **clear interface** on page 137
- **display dhcp-client** on page 148
- **display interface** on page 152

**set interface
dhcp-server**

Configures the MSS DHCP server.



Use of the MSS DHCP server to allocate client addresses is intended for temporary, demonstration deployments and not for production networks. It is recommended that you do not use the MSS DHCP server to allocate client addresses in a production network.

Syntax — `set interface vlan-id ip dhcp-server [enable | disable][start ip-addr1 stop ip-addr2][dns-domain domain-name][primary-dns ip-addr [secondary-dns ip-addr]] [default-router ip-addr]`

- `vlan-id` — VLAN name or number.
- **enable** — Enables the DHCP server.
- **disable** — Disables the DHCP server.
- **start** `ip-addr1` — Specifies the beginning address of the address range (also called the address *pool*).
- **stop** `ip-addr2` — Specifies the ending address of the address range.
- **dns-domain** `domain-name` — Name of the DHCP client's default DNS domain.
- **primary-dns** `ip-addr` [**secondary-dns** `ip-addr`] — IP addresses of the DHCP client's DNS servers.
- **default-router** `ip-addr` — IP address of the DHCP client's default router.

Defaults — The DHCP server is enabled by default on a new (unconfigured) WXR100, in order to provide an IP address to the host connected to the WX for access to the Web Quick Start. On all switch models, the DHCP server is enabled and cannot be disabled for directly connected MAPs.

The DHCP server is disabled by default for any other use.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — By default, all addresses except the host address of the VLAN, the network broadcast address, and the subnet broadcast address are included in the range. If you specify the range, the start address must be lower than the stop address, and all addresses must be in the same subnet. The IP interface of the VLAN must be within the same subnet but is not required to be within the range.

Examples — The following command enables the DHCP server on VLAN *red-vlan* to serve addresses from the 192.168.1.5 to 192.168.1.25 range:

```
WX1200# set interface red-vlan ip dhcp-server enable start
192.168.1.5 stop 192.168.1.25
success: change accepted.
```

See Also

- **display dhcp-server** on page 150
- **set ip dns domain** on page 175
- **set ip dns server** on page 176

set interface status

Administratively disables or reenables an IP interface.

Syntax — `set interface vlan-id status {up | down}`

- *vlan-id* — VLAN name or number.
- **up** — Enables the interface.
- **down** — Disables the interface.

Defaults — IP interfaces are enabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command disables the IP interface on VLAN mauve:

```
WX4400# set interface mauve status down
success: set interface mauve to down
```

See Also

- **clear interface** on page 137
- **display interface** on page 152
- **set interface** on page 170

set ip alias

Configures an alias, which maps a name to an IP address. You can use aliases as shortcuts in CLI commands.

Syntax — `set ip alias name ip-addr`

- *name* — String of up to 32 alphanumeric characters, with no spaces.
- *ip-addr* — IP address in dotted decimal notation.

Defaults — None.

Access — Enabled.

History— Introduced in MSS Version 3.0.

Examples — The following command configures the alias HR1 for IP address 192.168.1.2:

```
WX4400# set ip alias HR1 192.168.1.2
success: change accepted.
```

See Also

- **clear ip alias** on page 138
- **display ip alias** on page 153

set ip dns

Enables or disables DNS on a wireless LAN switch.

Syntax — `set ip dns {enable | disable}`

- **enable** — Enables DNS.
- **disable** — Disables DNS.

Defaults — DNS is disabled by default.

Access — Enabled.

History— Introduced in MSS Version 3.0.

Examples — The following command enables DNS on a WX switch:

```
WX1200# set ip dns enable
Start DNS Client
```

See Also

- **clear ip dns domain** on page 139
- **clear ip dns server** on page 139
- **display ip dns** on page 154
- **set ip dns domain** on page 175
- **set ip dns server** on page 176

set ip dns domain

Configures a default domain name for DNS queries. The WX appends the default domain name to domain names or hostnames you enter in commands.

Syntax — `set ip dns domain name`

- *name* — Domain name of between 1 and 64 alphanumeric characters with no spaces (for example, example.org).

Defaults — None.

Access — Enabled.

Usage — To override the default domain name when entering a hostname in a CLI command, enter a period at the end of the hostname. For example, if the default domain name is *example.com*, enter **chris.** if the fully qualified hostname is *chris* and not *chris.example.com*.

Aliases take precedence over DNS. When you enter a hostname, MSS checks for an alias with that name first, before using DNS to resolve the name.

Examples — The following command configures the default domain name *example.com*:

```
WX1200# set ip dns domain example.com
Domain name changed
```

See Also

- **clear ip dns domain** on page 139
- **clear ip dns server** on page 139
- **display ip dns** on page 154
- **set ip dns** on page 175
- **set ip dns server** on page 176

set ip dns server

Specifies a DNS server to use for resolving hostnames you enter in CLI commands.

Syntax — `set ip dns server ip-addr {primary | secondary}`

- *ip-addr* — IP address of a DNS server, in dotted decimal or CIDR notation.
- **primary** — Makes the server the primary server, which MSS always consults first for resolving DNS queries.
- **secondary** — Makes the server a secondary server. MSS consults a secondary server only if the primary server does not reply.

Defaults — None.

Access — Enabled.

Usage — You can configure a WX to use one primary DNS server and up to five secondary DNS servers.

Examples — The following commands configure a WX to use a primary DNS server and two secondary DNS servers:

```
WX1200# set ip dns server 10.10.10.50/24 primary
success: change accepted.
WX1200# set ip dns server 10.10.20.69/24 secondary
```



```

success: change accepted.
WX1200# set ip dns server 10.10.30.69/24 secondary
success: change accepted.

```

See Also

- **clear ip dns domain** on page 139
- **clear ip dns server** on page 139
- **display ip dns** on page 154
- **set ip dns** on page 175
- **set ip dns domain** on page 175

set ip https server

Enables the HTTPS server on a WX. The HTTPS server is required for Web View access to the switch.



CAUTION: *If you disable the HTTPS server, Web View access to the WX switch is also disabled.*

Syntax — `set ip https server {enable | disable}`

- **enable** — Enables the HTTPS server.
- **disable** — Disables the HTTPS server.

Defaults — The HTTPS server is disabled by default.

Access — Enabled.

History — The default is changed to disabled in 3.1. In addition, the HTTPS server is no longer required for WebAAA.

Examples — The following command enables the HTTPS server on a WX switch:

```

WX1200# set ip https server enable
success: change accepted.

```

See Also

- **clear ip telnet** on page 141
- **display ip https** on page 155
- **display ip telnet** on page 158
- **set ip telnet** on page 181
- **set ip telnet server** on page 182

set ip route

Adds a static route to the IP route table.

Syntax — `set ip route {default | ip-addr mask | ip-addr/mask-length} gateway metric`

- **default** — Default route. A WX switch uses the default route if an explicit route is not available for the destination.



Default is an alias for IP address 0.0.0.0/0.

- *ip-addr mask* — IP address and subnet mask for the route destination, in dotted decimal notation (for example, 10.10.10.10 255.255.255.0).
- *ip-addr/mask-length* — IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24).
- *gateway* — IP address, DNS hostname, or alias of the next-hop router.
- *metric* — Cost for using the route. You can specify a value from 0 through 2,147,483,647. Lower-cost routes are preferred over higher-cost routes.

Defaults — The HTTPS server is enabled by default.

Access — Enabled.

Usage — MSS can use a static route only if a direct route in the route table resolves the static route. MSS adds routes with next-hop types Local and Direct when you add an IP interface to a VLAN, if the VLAN is up. If one of these added routes can resolve the static route, MSS can use the static route.

Before you add a static route, use the **display interface** command to verify that the WX switch has an IP interface in the same subnet as the route's next-hop router. If not, the VLAN:Interface field of the **display ip route** command output shows that the route is down.

You can configure a maximum of 4 routes per destination. This includes default routes, which have destination 0.0.0.0/0. Each route to a given destination must have a unique gateway address. When the route table contains multiple default or explicit routes to the same destination, MSS uses the route with the lowest cost. If two or more routes to the same destination have the lowest cost, MSS selects the first route in the route table.

When you add multiple routes to the same destination, MSS groups the routes and orders them from lowest cost at the top of the group to highest cost at the bottom of the group. If you add a new route that has the same destination and cost as a route already in the table, MSS places the new route at the top of the group of routes with the same cost.

Examples — The following command adds a default route that uses gateway 10.5.4.1 and gives the route a cost of 1:

```
WX4400# set ip route default 10.5.4.1 1
success: change accepted.
```

The following commands add two default routes, and configure MSS to always use the route through 10.2.4.69 when the interface to that gateway router is up:

```
WX4400# set ip route default 10.2.4.69 1
success: change accepted.
WX4400# set ip route default 10.2.4.17 2
success: change accepted.
```

The following command adds an explicit route from a WX to any host on the 192.168.4.x subnet through the local router 10.5.4.2, and gives the route a cost of 1:

```
WX4400# set ip route 192.168.4.0 255.255.255.0 10.5.4.2 1
success: change accepted.
```

The following command adds another explicit route, using CIDR notation to specify the subnet mask:

```
WX4400# set ip route 192.168.5.0/24 10.5.5.2 1
success: change accepted.
```

See Also

- **clear ip route** on page 140
- **display interface** on page 152
- **display ip route** on page 156

set ip snmp server

Enables or disables the SNMP service on the WX.

Syntax — `set ip snmp server {enable | disable}`

enable — Enables the SNMP service.

disable — Disables the SNMP service.

Defaults — The SNMP service is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command enables the SNMP server on a WX switch:

```
WX4400# set ip snmp server enable
success: change accepted.
```

See Also

- **set port trap** on page 96
- **set snmp community** on page 185

set ip ssh

Changes the TCP port number on which a WX listens for Secure Shell (SSH) management traffic.



CAUTION: *If you change the SSH port number from an SSH session, MSS immediately ends the session. To open a new management session, you must configure the SSH client to use the new TCP port number.*

Syntax — `set ip ssh port port-num`

- *port-num* — TCP port number.

Defaults — The default SSH port number is 22.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command changes the SSH port number on a WX switch to 6000:

```
WX4400# set ip ssh port 6000
success: change accepted.
```

See Also

- **set ip ssh server** on page 181

set ip ssh server

Disables or reenables the SSH server on a WX.



CAUTION: *If you disable the SSH server, SSH access to the WX is also disabled.*

Syntax — `set ip ssh server {enable | disable}`

- **enable** — Enables the SSH server.
- **disable** — Disables the SSH server.

Defaults — The SSH server is enabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must generate an SSH authentication key to use SSH.

The maximum number of SSH sessions supported on a WX is eight. If Telnet is also enabled, the WX can have up to eight Telnet or SSH sessions, in any combination, and one Console session.

See Also

- **crypto generate key** on page 565
- **set ip ssh** on page 180
- **set ip ssh server** on page 181

set ip telnet

Changes the TCP port number on which a WX listens for Telnet management traffic.



CAUTION: *If you change the Telnet port number from a Telnet session, MSS immediately ends the session. To open a new management session, you must Telnet to the WX with the new Telnet port number.*

Syntax — `set ip telnet port-num`

- *port-num* — TCP port number.

Defaults — The default Telnet port number is 23.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command changes the Telnet port number on a WX to 5000:

```
WX4400# set ip telnet 5000
success: change accepted.
```

See Also

- **clear ip telnet** on page 141
- **display ip https** on page 155
- **display ip telnet** on page 158
- **set ip https server** on page 177
- **set ip telnet server** on page 182

set ip telnet server Enables the Telnet server on a WX.



CAUTION: *If you disable the Telnet server, Telnet access to the WX is also disabled.*

Syntax — `set ip telnet server {enable | disable}`

- **enable** — Enables the Telnet server.
- **disable** — Disables the Telnet server.

Defaults — The Telnet server is disabled by default.

Access — Enabled.

Usage — The maximum number of Telnet sessions supported on a WX is eight. If SSH is also enabled, the WX can have up to eight Telnet or SSH sessions, in any combination, and one console session.

Examples — The following command enables the Telnet server on a WX:

```
WX4400# set ip telnet server enable
success: change accepted.
```

See Also

- **clear ip telnet** on page 141
- **display ip https** on page 155
- **display ip telnet** on page 158
- **set ip https server** on page 177
- **set ip telnet** on page 181

set ntp

Enables or disables the NTP client on a WX.

Syntax — `set ntp {enable | disable}`

- **enable** — Enables the NTP client.
- **disable** — Disables the NTP client.

Defaults — The NTP client is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — If NTP is configured on a system whose current time differs from the NTP server time by more than 10 minutes, convergence of the WX time can take many NTP update intervals. 3Com recommends that you set the time manually to the NTP server time before enabling NTP to avoid a significant delay in convergence.

Examples — The following command enables the NTP client:

```
WX4400# set ntp enable
success: NTP Client enabled
```

See Also

- **clear ntp server** on page 141
- **clear ntp update-interval** on page 142
- **display ntp** on page 159
- **set ntp server** on page 184
- **set ntp update-interval** on page 185

set ntp server

Configures a WX to use an NTP server.

Syntax — `set ntp server ip-addr`

- *ip-addr* — IP address of the NTP server, in dotted decimal notation.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You can configure up to three NTP servers. MSS queries all the servers and selects the best response based on the method described in RFC 1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis.

To use NTP, you also must enable the NTP client with the **set ntp** command.

Examples — The following command configures a WX switch to use NTP server 192.168.1.5:

```
WX4400# set ntp server 192.168.1.5
```

See Also

- **clear ntp server** on page 141
- **clear ntp update-interval** on page 142
- **display ntp** on page 159
- **set ntp** on page 183
- **set ntp update-interval** on page 185

set ntp update-interval

Changes how often a WX sends queries to the NTP servers for updates.

Syntax — `set ntp update-interval seconds`

- *seconds* — Number of seconds between queries. You can specify from 16 through 1,024 seconds.

Defaults — The default NTP update interval is 64 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command changes the NTP update interval to 128 seconds:

```
WX4400# set ntp update-interval 128
success: change accepted.
```

See Also

- **clear ntp server** on page 141
- **clear ntp update-interval** on page 142
- **display ntp** on page 159
- **set ntp** on page 183
- **set ntp server** on page 184

set snmp community



Configures a community string for SNMPv1 or SNMPv2c.

For SNMPv3, use the **set snmp usm** command to configure an SNMPv3 user. SNMPv3 does not use community strings.

Syntax — `set snmp community comm-string`

`access {read-only / read-notify / notify-only / read-write / notify-read-write}`

- *comm-string* — Name of the SNMP community. Specify between 1 and 32 alphanumeric characters, with no spaces.
- **read-only** — Allows an SNMP management application using the string to get (read) object values on the switch but not to set (write) them.

- **read-notify** — Allows an SNMP management application using the string to get object values on the switch but not to set them. The switch can use the string to send notifications.
- **notify-only** — Allows the WX to use the string to send notifications.
- **read-write** — Allows an SNMP management application using the string to get and set object values on the switch.
- **notify-read-write** — Allows an SNMP management application using the string to get and set object values on the switch. The switch also can use the string to send notifications.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. Default community strings changed from *public* (for read-only) and *private* (for read-write) to blank in MSS Version 3.1. Default strings removed and new access types added for SNMPv3 (read-notify, notify-only, notify-read-write) in MSS Version 4.0.

Usage — SNMP community strings are passed as clear text in SNMPv1 and SNMPv2c. 3Com recommends that you use strings that cannot easily be guessed by unauthorized users. For example, do not use the well-known strings *public* and *private*.

If you are using SNMPv3, you can configure SNMPv3 users to use authentication and to encrypt SNMP data.

Examples — The following command configures the read-write community *good_community*:

```
WX4400# set snmp community read-write good_community
success: change accepted.
```

The following command configures community string *switchmgr1* with access level notify-read-write:

```
WX4400# set snmp community name switchmgr1 notify-read-write
success: change accepted.
```

See Also

- **clear snmp community** on page 143
- **set ip snmp server** on page 180
- **set snmp notify target** on page 192
- **set snmp notify profile** on page 187
- **set snmp protocol** on page 197
- **set snmp security** on page 198
- **set snmp usm** on page 199
- **display snmp community** on page 161

set snmp notify profile

Configures an SNMP notification profile. A *notification profile* is a named list of all the notification types that can be generated by a switch, and for each notification type, the action to take (drop or send) when an event occurs.

You can configure up to ten notification profiles.

Syntax — `set snmp notify profile {default | profile-name} {drop | send} {notification-type | all}`

- **default | profile-name** — Name of the notification profile you are creating or modifying. The profile-name can be up to 32 alphanumeric characters long, with no spaces. To modify the default notification profile, specify **default**.
- **drop | send** — Specifies the action that the SNMP engine takes with regard to the notifications you specify with notification-type or all.
- **notification-type** — Name of the notification type:
 - **APBootTraps**—Generated when a MAP access point boots.
 - **ApNonOperStatusTraps**—Generated to indicate a MAP radio is nonoperational.
 - **ApOperRadioStatusTraps**—Generated when the status of a MAP radio changes.
 - **APRejectLicenseExceededTraps**—Generated when a WX switch receives a packet from an inactive AP and attaching that AP would make the WX switch exceed the maximum (licensed) number of active APs.

- **APTimeoutTraps**—Generated when a MAP access point fails to respond to the WX switch.
- **AuthenTraps**—Generated when the WX switch’s SNMP engine receives a bad community string.
- **AutoTuneRadioChannelChangeTraps**—Generated when the RF Auto-Tuning feature changes the channel on a radio.
- **AutoTuneRadioPowerChangeTraps**—Generated when the RF Auto-Tuning feature changes the power setting on a radio.
- **ClientAssociationFailureTraps**—Generated when a client’s attempt to associate with a radio fails.
- **ClientAssociationSuccessTraps**—Generated when a client is successfully associated.
- **ClientAuthorizationSuccessTraps**—Generated when a client is successfully authorized.
- **ClientAuthenticationFailureTraps**—Generated when authentication fails for a client.
- **ClientAuthenticationSuccessTraps**—Generated when a client is successfully authenticated.
- **ClientAuthorizationFailureTraps**—Generated when authorization fails for a client.
- **ClientClearedTraps**—Generated when a client’s session is cleared.
- **ClientDeAssociationTraps**—Generated when a client is dissociated from a radio.
- **ClientDeAuthenticationTraps**—Generated when a client is disauthenticated from a radio.
- **ClientDot1xFailureTraps**—Generated when a client experiences an 802.1X failure.
- **ClientIpAddressChangeTraps**—Generated when a client’s IP address changes.
- **ClientRoamingTraps**—Generated when a client roams.
- **CounterMeasureStartTraps**—Generated when MSS begins countermeasures against a rogue access point.
- **CounterMeasureStopTraps**—Generated when MSS stops countermeasures against a rogue access point.

- **DAPConnectWarningTraps**—Generated when a Distributed MAP whose fingerprint has not been configured in MSS establishes a management session with the switch.
- **DeviceFailTraps**—Generated when an event with an Alert severity occurs.
- **DeviceOkayTraps**—Generated when a device returns to its normal state.
- **LinkDownTraps**—Generated when the link is lost on a port.
- **LinkUpTraps**—Generated when the link is detected on a port.
- **MichaelMICFailureTraps**—Generated when two Michael message integrity code (MIC) failures occur within 60 seconds, triggering Wi-Fi Protected Access (WPA) countermeasures.
- **MobilityDomainJoinTraps**—Generated when the WX switch is initially able to contact a mobility domain seed member, or can contact the seed member after a timeout.
- **MobilityDomainTimeoutTraps**—Generated when a timeout occurs after a WX switch has unsuccessfully tried to communicate with a seed member.
- **PoEFailTraps**—Generated when a serious PoE problem, such as a short circuit, occurs.
- **RFDetectAdhocUserTraps**—Generated when MSS detects an ad-hoc user.
- **RFDetectAdhocUserDisappearTraps**—Generated when an ad-hoc user is no longer being detected.
- **RFDetectBlacklistedTraps**—Generated when an association, re-association, or deassociation request is detected from a blacklisted transmitter.
- **RFDetectRogueAPTraps**—Generated when MSS detects a rogue access point.
- **RFDetectRogueDisappearTraps**—Generated when a rogue access point is no longer being detected.
- **RFDetectClientViaRogueWiredAPTraps**—Generated when MSS detects, on the wired part of the network, the MAC address of a wireless client associated with a third-party AP.

- **RFDetectDoSportTraps**—Generated when MSS detects an associate request flood, reassociate request flood, or disassociate request flood.
- **RFDetectDoSTraps**—Generated when MSS detects a DoS attack other than an associate request flood, reassociate request flood, or disassociate request flood.
- **RFDetectInterferingRogueAPTraps**—Generated when an interfering device is detected.
- **RFDetectInterferingRogueDisappearTraps**—Generated when an interfering device is no longer detected.
- **RFDetectSpoofedMacAPTraps**—Generated when MSS detects a wireless packet with the source MAC address of a MAP, but without the spoofed MAP's signature (fingerprint).
- **RFDetectSpoofedSsidAPTraps**—Generated when MSS detects beacon frames for a valid SSID, but sent by a rogue AP.
- **RFDetectUnauthorizedAPTraps**—Generated when MSS detects the MAC address of a MAP that is on the attack list.
- **RFDetectUnauthorizedOuiTraps**—Generated when a wireless device that is not on the list of permitted vendors is detected.
- **RFDetectUnauthorizedSsidTraps**—Generated when an SSID that is not on the permitted SSID list is detected.
- **a11** — Sends or drops all notifications.

Defaults — A default notification profile (named *default*) is already configured on the WX. All notifications in the default profile are dropped by default.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command changes the action in the default notification profile from **drop** to **send** for all notification types:

```
WX1200# set snmp notify profile default send all
success: change accepted.
```

The following commands create notification profile *snmpprof_rfdetect*, and change the action to **send** for all RF detection notification types:

```
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectAdhocUserTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectAdhocUserDisappearTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectBlacklistedUserTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectClientViaRogueWiredAPTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectDoSTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectAdhocUserTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectInterferingRogueAPTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectInterferingRogueDisappearTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectRogueAPTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectRogueDisappearTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectSpoofedMacAPTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectSpoofedSsidAPTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectUnauthorizedAPTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectUnauthorizedOuiTraps
success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send
RFDetectUnauthorizedSsidTraps
success: change accepted.
```

See Also

- **clear snmp notify profile** on page 143
- **set ip snmp server** on page 180
- **set snmp community** on page 185
- **set snmp notify target** on page 192
- **set snmp protocol** on page 197
- **set snmp security** on page 198
- **set snmp usm** on page 199
- **set snmp notify profile** on page 187

set snmp notify target

Configures a notification target for notifications from SNMP.

A notification target is a remote device that the WX sends SNMP notifications. You can configure the MSS SNMP engine to send confirmed notifications (informs) or unconfirmed notifications (traps). Some of the command options differ depending on the SNMP version and the type of notification you specify. You can configure up to 10 notification targets.

SNMPv3 with Informs

To configure a notification target for informs from SNMPv3, use the following command:

Syntax — **set snmp notify target** *target-num*
ip-addr[:udp-port-number]
usm inform user *username*
snmp-engine-id {**ip** | **hex** *hex-string*}
[**profile** *profile-name*]
[**security** {**unsecured** | **authenticated** | **encrypted**}]
[**retries** *num*]
[**timeout** *num*]

- *target-num* — ID for the target. This ID is local to the WX switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
- *ip-addr[:udp-port-number]* — IP address of the server. You also can specify the UDP port number to send notifications to.

- *username* — USM username. This option is applicable only when the SNMP version is **usm**. If the user will send informs rather than traps, you also must specify the **snmp-engine-id** of the target.
- **snmp-engine-id** — SNMP engine ID of the target. Specify *ip* if the target SNMP engine ID is based on its IP address. If the target's SNMP engine ID is a hexadecimal value, use *hex hex-string* to specify the value.
- **profile** *profile-name* — Notification profile that this SNMP user will use to specify the notification types to send or drop.
- **security** — Specifies the security level, and is applicable only when the SNMP version is **usm**:
 - {unsecured | authenticated | encrypted}**
 - **unsecured** — Message exchanges are not authenticated, nor are they encrypted. This is the default.
 - **authenticated** — Message exchanges are authenticated, but are not encrypted.
 - **encrypted** — Message exchanges are authenticated and encrypted.
- **retries** *num* — Specifies the number of times the MSS SNMP engine will resend a notification that has not been acknowledged by the target. You can specify from 0 to 3 retries.
- **timeout** *num* — Specifies the number of seconds MSS waits for acknowledgement of a notification. You can specify from 1 to 5 seconds.

SNMPv3 with Traps

To configure a notification target for traps from SNMPv3, use the following command:

```
Syntax — set snmp notify target target-num ip-addr[:udp-port-number]
usm trap user username
[profile profile-name]
[security {unsecured | authenticated | encrypted}]
```

- **target-num** — ID for the target. This ID is local to the WX switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
- **ip-addr[:udp-port-number]** — IP address of the server. You also can specify the UDP port number to send notifications to.

- **username** — USM username. This option is applicable only when the SNMP version is **usm**.
- **profile profile-name** — Notification profile this SNMP user will use to specify the notification types to send or drop.
- **security** — Specifies the security level, and is applicable only when the SNMP version is **usm**:
 - {**unsecured** | **authenticated** | **encrypted**}
 - **unsecured** — Message exchanges are not authenticated, nor are they encrypted. This is the default.
 - **authenticated** — Message exchanges are authenticated, but are not encrypted.
 - **encrypted** — Message exchanges are authenticated and encrypted.

SNMPv2c with Informs

To configure a notification target for informs from SNMPv2c, use the following command:

```
Syntax — set snmp notify target target-num ip-addr[:udp-port-number]
v2c community-string inform
[profile profile-name]
[retries num]
[timeout num]
```

- **target-num** — ID for the target. This ID is local to the WX switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
- *ip-addr[:udp-port-number]* — IP address of the server. You also can specify the UDP port number to send notifications to.
- *community-string* — Community string.
- **profile profile-name** — Notification profile this SNMP user will use to specify the notification types to send or drop.
- **retries num** — Notification profile this SNMP user will use to specify the notification types to send or drop.
- **timeout num** — Specifies the number of seconds MSS waits for acknowledgement of a notification. You can specify from 1 to 5 seconds.

SNMPv2c with Traps

To configure a notification target for traps from SNMPv2c, use the following command:

Syntax — `set snmp notify target target-num ip-addr[:udp-port-number] v2c community-string trap [profile profile-name]`

- *target-num* — ID for the target. This ID is local to the WX switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
- *ip-addr[:udp-port-number]* — IP address of the server. You also can specify the UDP port number to send notifications to.
- *community-string* — Community string.
- **profile** *profile-name* — Notification profile this SNMP user will use to specify the notification types to send or drop.

SNMPv1 with Traps

To configure a notification target for traps from SNMPv1, use the following command:

Syntax — `set snmp notify target target-num ip-addr[:udp-port-number] v1 community-string [profile profile-name]`

- *target-num* — ID for the target. This ID is local to the WX switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
- *ip-addr[:udp-port-number]* — IP address of the server. You also can specify the UDP port number to send notifications to.
- *community-string* — Community string.
- **profile** *profile-name* — Notification profile this SNMP user will use to specify the notification types to send or drop.

Defaults — The default UDP port number on the target is 162. The default minimum required security level is **unsecured**. The default number of retries is 0 and the default timeout is 2 seconds.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — The **inform** or **trap** option specifies whether the MSS SNMP engine expects the target to acknowledge notifications sent to the target by the WX switch. Use **inform** if you want acknowledgements. Use **trap** if you do not want acknowledgements. The **inform** option is applicable to SNMP version **v2c** or **usm** only.

Examples — The following command configures a notification target for acknowledged notifications:

```
WX1200# set snmp notify target 1 10.10.40.9 usm inform user
securesnmpmgr1 snmp-engine-id ip
success: change accepted.
```

This command configures target 1 at IP address 10.10.40.9. The target's SNMP engine ID is based on its address. The MSS SNMP engine will send notifications based on the default profile, and will require the target to acknowledge receiving them.

The following command configures a notification target for unacknowledged notifications:

```
WX1200# set snmp notify target 2 10.10.40.10 v1 trap
success: change accepted.
```

See Also

- **clear snmp notify target** on page 144
- **set ip snmp server** on page 180
- **set snmp community** on page 185
- **set snmp notify profile** on page 187
- **set snmp protocol** on page 197
- **set snmp security** on page 198
- **set snmp usm** on page 199
- **display snmp notify target** on page 162

set snmp protocol

Enables an SNMP protocol. MSS supports SNMPv1, SNMPv2c, and SNMPv3.

Syntax — `set snmp protocol {v1 | v2c | usm | all} {enable | disable}`

- **v1** — SNMPv1
- **v2c** — SNMPv2c
- **usm** — SNMPv3 (with the user security model)
- **all** — Enables all supported versions of SNMP.
- **enable** — Enables the specified SNMP version(s).
- **disable** — Disables the specified SNMP version(s).

Defaults — All SNMP versions are disabled by default.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — SNMP requires the switch system IP address to be set. SNMP does not work without the system IP address.

You also must enable the SNMP service using the **set ip snmp server** command.

Examples — The following command enables all SNMP versions:

```
WX1200# set snmp protocol all enable
success: change accepted.
```

See Also

- **set ip snmp server** on page 180
- **set snmp community** on page 185
- **set snmp notify target** on page 192
- **set snmp security** on page 198
- **set snmp usm** on page 199
- **display snmp status** on page 163

set snmp security

Sets the minimum level of security MSS requires for SNMP message exchanges.

Syntax — `set snmp security`

`{unsecured | authenticated | encrypted | auth-req-unsec-notify}`

- **unsecured** — SNMP message exchanges are not secure. This is the only value supported for SNMPv1 and SNMPv2c.
- **authenticated** — SNMP message exchanges are authenticated but are not encrypted.
- **encrypted** — SNMP message exchanges are authenticated and encrypted.
- **auth-req-unsec-notify** — SNMP message exchanges are authenticated but are not encrypted, and notifications are neither authenticated nor encrypted.

Defaults — By default, MSS allows nonsecure (**unsecured**) SNMP message exchanges.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — SNMPv1 and SNMPv2c do not support authentication or encryption. If you plan to use SNMPv1 or SNMPv2c, leave the minimum level of SNMP security set to **unsecured**.

Examples — The following command sets the minimum level of SNMP security allowed to authentication *and* encryption:

```
WX1200# set snmp security encrypted
success: change accepted.
```

See Also

- **set ip snmp server** on page 180
- **set snmp community** on page 185
- **set snmp notify target** on page 192
- **set snmp notify profile** on page 187
- **set snmp protocol** on page 197

- **set snmp usm** on page 199
- **display snmp status** on page 163

set snmp usm

Creates a USM user for SNMPv3.



*This command does not apply to SNMPv1 or SNMPv2c. For these SNMP versions, use the **set snmp community** command to configure community strings.*

Syntax — `set snmp usm usm-username
snmp-engine-id {ip ip-addr | local | hex hex-string}
access {read-only | read-notify | notify-only | read-write |
notify-read-write}
auth-type {none | md5 | sha} {auth-pass-phrase string |
auth-key hex-string}
encrypt-type {none | des | 3des | aes} {encrypt-pass-phrase
string | encrypt-key hex-string}`

- **usm-username** — Name of the SNMPv3 user. Specify between 1 and 32 alphanumeric characters, with no spaces.
- **snmp-engine-id {ip ip-addr | local | hex hex-string}** — Specifies a unique identifier for the SNMP engine. To send informs, you must specify the engine ID of the inform receiver. To send traps and to allow get and set operations and so on, specify local as the engine ID.
 - **hex hex-string**—ID is a hexadecimal string.
 - **ip ip-addr**—ID is based on the IP address of the station running the management application. Enter the IP address of the station. MSS calculates the engine ID based on the address.
 - **local** — Uses the value computed from the switch's system IP address.
- **access {read-only | read-notify | notify-only | read-write | notify-read-write}** — Specifies the access level of the user:
 - **read-only**—An SNMP management application using the string can get (read) object values on the switch but cannot set (write) them.
 - **read-notify**—An SNMP management application using the string can get object values on the switch but cannot set them. The switch can use the string to send notifications.

- **notify-only**—The switch can use the string to send notifications.
- **read-write**—An SNMP management application using the string can get and set object values on the switch.
- **notify-read-write** — An SNMP management application using the string can get and set object values on the switch. The switch can use the string to send notifications.
- **auth-type {none | md5 | sha} {auth-pass-phrase string | auth-key hex-string}** — Specifies the authentication type used to authenticate communications with the remote SNMP engine. You can specify one of the following:
 - **none**—No authentication is used.
 - **md5**—Message-digest algorithm 5 is used.
 - **sha**—Secure Hashing Algorithm (SHA) is used.

If the authentication type is **md5** or **sha**, you can specify a passphrase or a hexadecimal key.

- To specify a passphrase, use the **auth-pass-phrase string** option. The string can be from 8 to 32 alphanumeric characters long, with no spaces.
 - To specify a key, use the **auth-key hex-string** option.
- **encrypt-type {none | des | 3des | aes} {encrypt-pass-phrase string | encrypt-key hex-string}** — Specifies the encryption type used for SNMP traffic. You can specify one of the following:
 - **none**—No encryption is used. This is the default.
 - **des**—Data Encryption Standard (DES) encryption is used.
 - **3des**—Triple DES encryption is used.
 - **aes**—Advanced Encryption Standard (AES) encryption is used.

If the encryption type is **des**, **3des**, or **aes**, you can specify a passphrase or a hexadecimal key.

 - To specify a passphrase, use the **encrypt-pass-phrase string** option. The string can be from 8 to 32 alphanumeric characters long, with no spaces.
 - To specify a key, use the **encrypt-key hex-string** option.

Defaults — No SNMPv3 users are configured by default. When you configure an SNMPv3 user, the default access is **read-only**, and the default authentication and encryption types are both **none**.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command creates USM user *snmpmgr1*, associated with the local SNMP engine ID. This user can send traps to notification receivers.

```
WX#1200 set snmp usm snmpmgr1 snmp-engine-id local
success: change accepted.
```

The following command creates USM user *securesnmpmgr1*, which uses SHA authentication and 3DES encryption with passphrases. This user can send informs to the notification receiver that has engine ID 192.168.40.2.

```
WX4400# set snmp usm securesnmpmgr1 snmp-engine-id ip
192.168.40.2 auth-type sha auth-pass-phrase myauthpwd
encrypt-type 3des encrypt-pass-phrase mycryptpwd
success: change accepted.
```

See Also

- **clear snmp usm** on page 144
- **set ip snmp server** on page 180
- **set snmp community** on page 185
- **set snmp notify target** on page 192
- **set snmp notify profile** on page 187
- **set snmp protocol** on page 197
- **set snmp security** on page 198
- **display snmp usm** on page 164

set summertime

Offsets the real-time clock of a WX by +1 hour and returns it to standard time for daylight savings time or a similar summertime period.

Syntax — `set summertime summer-name [start week weekday month hour min end week weekday month hour min]`

- *summer-name* — Name of up to 32 alphanumeric characters that describes the summertime offset. You can use a standard name or any name you like.
- **start** — Start of the time change period.
- *week* — Week of the month to start or end the time change. Valid values are **first, second, third, fourth,** or **last**.
- *weekday* — Day of the week to start or end the time change. Valid values are **sun, mon, tue, wed, thu, fri,** and **sat**.
- *month* — Month of the year to start or end the time change. Valid values are **jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov,** and **dec**.
- *hour* — Hour to start or end the time change — a value between 0 and 23 on the 24-hour clock.
- *min* — Minute to start or end the time change — a value between 0 and 59.
- **end** — End of the time change period.

Defaults — If you do not specify a start and end time, the system implements the time change starting at 2:00 a.m. on the first Sunday in April and ending at 2:00 a.m. on the last Sunday in October, according to the North American standard.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must first set the time zone with the **set timezone** command for the offset to work properly without the **start** and **end** values.

Configure summertime before you set the time and date. Otherwise, summertime's adjustment of the time will make the time incorrect, if the date is within the summertime period.

Examples — To enable summertime and set the summertime time zone to PDT (Pacific Daylight Time), type the following command:

```
WX1200# set summertime PDT
success: change accepted
```

See Also

- **clear summertime** on page 145
- **clear timezone** on page 146
- **display summertime** on page 164
- **display timedate** on page 165
- **display timezone** on page 165
- **set timedate** on page 204
- **set timezone** on page 205

set system ip-address

Configures the system IP address. The system IP address determines the interface or source IP address MSS uses for system tasks, including the following:

- Mobility domain operations
- Topology reporting for dual-homed MAP access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Syntax — `set system ip-address ip-addr`

- *ip-addr* — IP address, in dotted decimal notation. The address must be configured on one of the WX VLANs.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must use an address that is configured on one of the WX switch VLANs.

To display the system IP address, use the **display system** command.

Examples — The following commands configure an IP interface on VLAN taupe and configure the interface to be the system IP address:

```
WX4400# set interface taupe ip 10.10.20.20/24
success: set ip address 10.10.20.20 netmask 255.255.255.0 on vlan taupe
WX4400# set system ip-address 10.10.20.20
success: change accepted.
```

See Also

- **clear system ip-address** on page 146
- **display system** on page 47
- **set interface** on page 170

set timedate

Sets the time of day and date on the WX.

Syntax — `set timedate {date mmm dd yyyy [time hh:mm:ss]}`

- **date** *mmm dd yyyy* — System date:
 - *mmm* — month
 - *dd* — day
 - *yyyy* — year
- **time** *hh:mm:ss* — System time, in hours, minutes, and seconds.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The day of week is automatically calculated from the day that you set. The time displayed by the CLI after you type the command might be slightly later than the time you enter due to the interval between when you press Enter and when the CLI reads and displays the new time and date.

Configure summertime *before* you set the time and date. Otherwise, the summertime adjustment makes the time incorrect, if the date is within the summertime period.

Examples — The following command sets the date to March 13, 2003 and time to 11:11:12:

```
WX4400# set timedate date feb 29 2004 time 23:58:00
Time now is:                Sun Feb 29 2004, 23:58:02 PST
```

See Also

- **clear summertime** on page 145
- **clear timezone** on page 146
- **display summertime** on page 164
- **display timedate** on page 165
- **display timezone** on page 165
- **set summertime** on page 202
- **set timezone** on page 205

set timezone

Sets the number of hours, and optionally the number of minutes, that the WX real-time clock is offset from Coordinated Universal Time (UTC). These values are also used by Network Time Protocol (NTP), if it is enabled.

Syntax — `set timezone zone-name {-hours [minutes]}`

- *zone-name* — Time zone name of up to 32 alphabetic characters. You can use a standard name or any name you like.
- - (minus sign) — Minus time to indicate hours (and minutes) to be subtracted from UTC. Otherwise, hours and minutes are added by default.
- *hours* — Number of hours to add or subtract from UTC.
- *minutes* — Number of minutes to add or subtract from UTC.

Defaults — If this command is not used, then the default time zone is UTC.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To set the time zone for Pacific Standard Time (PST), type the following command:

```
WX1200# set timezone PST -8
Timezone is set to 'PST', offset from UTC is -8:0 hours.
```

See Also

- **clear summertime** on page 145
- **clear timezone** on page 146
- **display summertime** on page 164
- **display timedate** on page 165
- **display timezone** on page 165
- **set summertime** on page 202
- **set timedate** on page 204

telnet

Opens a Telnet client session with a remote device.

Syntax — `telnet {ip-addr | hostname} [port port-num]`

- *ip-addr* — IP address of the remote device.
- *hostname* — Hostname of the remote device.
- **port** *port-num* — TCP port number on which the TCP server on the remote device listens for Telnet connections.

Defaults — MSS attempts to establish Telnet connections with TCP port 23 by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To end a Telnet session from the remote device, press **Ctrl+t** or type **quit** or **logout** in the management session on the remote device. To end a client session from the local WX switch, use the **clear sessions telnet client** command.

If the configuration of the WX switch from which you enter the **telnet** command has an ACL that denies Telnet client traffic, the ACL also denies access by the **telnet** command.

Examples — In the following example, an administrator establishes a Telnet session with another device and enters a command on the remote device:

```
WX4400# telnet 10.10.10.90
Session 0 pty tty2.d Trying 10.10.10.90...
Connected to 10.10.10.90
Disconnect character is '^t'
```

Copyright (c) 2004 3Com Corporation. All rights reserved.

Username: **username**

Password: **password**

WX1200-remote> **display vlan**

VLAN Name	Admin Status	VLAN State	Tunl Affin	Port	Tag	Port State
1 default	Up	Up	5			
				3	none	Up
3 red	Up	Up	5			
10 backbone	Up	Up	5			
				1	none	Up
				2	none	Up
4094 web-aaa	Up	Up	0			
				2	4094	Up

When the administrator presses Ctrl+t to end the Telnet connection, the management session returns to the local prompt:

```
WX1200-remote> Session 0 pty tty2.d terminated tt name tty2.d
WX1200#
```

See Also

- **clear sessions** on page 613
- **display sessions** on page 616

tracert

Traces the route to an IP host.

Syntax — **tracert** *host* [**dnf**] [**no-dns**] [**port** *port-num*] [**queries** *num*] [**size** *size*] [**ttl** *hops*] [**wait** *ms*]

- *host* — IP address, hostname, or alias of the destination host. Specify the IP address in dotted decimal notation.

- **dnf** — Sets the Do Not Fragment bit in the ping packet to prevent the packet from being fragmented.
- **no-dns** — Prevents MSS from performing a DNS lookup for each hop to the destination host.
- **port** *port-num* — TCP port number listening for the traceroute probes.
- **queries** *num* — Number of probes per hop.
- **size** *size* — Probe packet size in bytes. You can specify from 40 through 1,460.
- **ttl** *hops* — Maximum number of hops, which can be from 1 through 255.
- **wait** *ms* — Probe wait in milliseconds. You can specify from 1 through 100,000.

Defaults

- **dnf** — Disabled
- **no-dns** — Disabled
- **port** — 33434
- **queries** — 3
- **size** — 38
- **ttl** — 30
- **wait** — 5000

Access — All.

History — Introduced in MSS Version 3.0.

Usage — To stop a traceroute command that is in progress, press **Ctrl+C**.

Examples — The following example traces the route to host server1:

```
WX4400# traceroute server1
traceroute to server1.example.com (192.168.22.7), 30 hops max, 38 byte packets
 1 engineering-1.example.com (192.168.192.206) 2 ms 1 ms 1 ms
 2 engineering-2.example.com (192.168.196.204) 2 ms 3 ms 2 ms
 3 gateway_a.example.com (192.168.1.201) 6 ms 3 ms 3 ms
 4 server1.example.com (192.168.22.7) 3 ms * 2 ms
```


The first row of the display indicates the target host, the maximum number of hops, and the packet size. Each numbered row displays information about one hop. The rows are displayed in the order in which the hops occur, beginning with the hop closest to the WX switch.

The row for a hop lists the total time in milliseconds for each ICMP packet to reach the router or host, plus the time for the ICMP Time Exceeded message to return to the host.

An exclamation point (!) following any of these values indicates that the Port Unreachable message returned by the destination has a maximum hop count of 0 or 1. This can occur if the destination uses the maximum hop count value from the arriving packet as the maximum hop count in its ICMP reply. The reply does not arrive at the source until the destination receives a traceroute packet with a maximum hop count equal to the number of hops between the source and destination.

An asterisk (*) indicates that the timeout period expired before MSS received a Time Exceeded message for the packet.

If Traceroute receives an ICMP error message other than a Time Exceeded or Port Unreachable message, MSS displays one of the error codes described in Table 40 instead of displaying the round-trip time or an asterisk (*).

Table 40 describes the traceroute error messages.

Table 40 Error messages for traceroute

Field	Description
!N	No route to host. The network is unreachable.
!H	No route to host. The host is unreachable.
!P	Connection refused. The protocol is unreachable.
!F	Fragmentation needed but Do Not Fragment (DNF) bit was set.
!S	Source route failed.
!A	Communication administratively prohibited.
?	Unknown error occurred.

See Also

- ping on page 166

8

AAA COMMANDS

Use authentication, authorization, and accounting (AAA) commands to provide a secure network connection and a record of user activity. Location policy commands override any virtual LAN (VLAN) or security ACL assignment by AAA or the local WX database to help you control access locally.

(Security ACLs are packet filters. For command descriptions, see Chapter 14.)

Commands by Usage

This chapter presents AAA commands alphabetically. Use Table 41 to locate commands in this chapter based on their use.

Table 41 AAA Commands by Usage

Type	Command
Authentication	set authentication console on page 241
	set authentication admin on page 239
	set authentication dot1x on page 243
	set authentication mac on page 247
	set authentication mac on page 247
	set authentication proxy on page 253
	clear authentication admin on page 214
	clear authentication console on page 215
	clear authentication dot1x on page 216
	clear authentication mac on page 217
	clear authentication mac on page 217
	clear authentication proxy on page 218
	clear authentication web on page 218

Table 41 AAA Commands by Usage (continued)

Type	Command
Local Authorization for Password Users	set user on page 271
	clear user on page 224
	set user attr on page 273
	clear user attr on page 225
	set usergroup on page 275
	clear usergroup on page 227
	set user group on page 275
	clear user group on page 226
	clear usergroup attr on page 228
Local Authorization for MAC Users	set mac-user on page 260
	clear mac-user on page 220
	set mac-user attr on page 261
	clear mac-user attr on page 221
	set mac-usergroup attr on page 267
	clear mac-usergroup attr on page 223
	clear mac-user group on page 221
clear mac-usergroup on page 222	
Web authorization	set web-portal on page 278
Accounting	set accounting {admin console} on page 235
	set accounting {dot1x mac web last-resort} on page 237
	display accounting statistics on page 232
	clear accounting on page 213
AAA information	display aaa on page 229
Mobility Profiles	set mobility-profile on page 269
	set mobility-profile mode on page 271
	display mobility-profile on page 235
Location Policy	clear mobility-profile on page 224
	set location policy on page 256
	display location policy on page 234
	clear location policy on page 219

Table 41 AAA Commands by Usage (continued)

Type	Command
Password and User Login Restrictions	set authentication password-restrict on page 252
	set authentication max-attempts on page 250
	set authentication minimum-password-length on page 251
	set user expire-password-in on page 274
	set usergroup expire-password-in on page 277
	clear user lockout on page 226

clear accounting

Removes accounting services for specified wireless users with administrative access or network access.

Syntax — `clear accounting {admin | dot1x} {user-glob}`

- **admin** — Users with administrative access to the WX through a console connection or through a Telnet or Web View connection.
- **dot1x** — Users with network access through the WX. Users with network access are authorized to use the network through either an IEEE 802.1X method or their media access control (MAC) address.
- **user-glob** — Single user or set of users with administrative access or network access.

Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see “User Globbs” on page 30.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes accounting services for authorized network user Nin:

```
WX4400# clear accounting dot1x Nin
success: change accepted.
```

See Also

- **set accounting {admin | console}** on page 235
- **display accounting statistics** on page 232

clear authentication admin

Removes an authentication rule for administrative access through Telnet or Web Manager.

Syntax — `clear authentication admin user-glob`

- *user-glob* — A single user or set of users.
Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character, either an at sign (@) or a period (.). (For details, see “User Globs” on page 30.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.



*The syntax descriptions for the **clear authentication** commands are separate for clarity. However, the options and behavior for the **clear authentication admin** command are the same as in previous releases.*

Examples — The following command clears authentication for administrator Jose:

```
WX4400# clear authentication admin Jose
success: change accepted.
```

See Also

- **clear authentication console** on page 215
- **clear authentication dot1x** on page 216

- **clear authentication mac** on page 217
- **clear authentication mac** on page 217
- **clear authentication proxy** on page 218
- **display aaa** on page 229
- **set authentication admin** on page 239

clear authentication console

Removes an authentication rule for administrative access through the Console.

Syntax — `clear authentication console user-glob`

- *user-glob* — A single user or set of users.

Specify a username, use the double-asterisk wildcard character (******) to specify all usernames, or use the single-asterisk wildcard character (*****) to specify a set of usernames up to or following the first delimiter character, either an *at* sign (**@**) or a period (**.**). (For details, see “User Globs” on page 30.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.



*The syntax descriptions for the **clear authentication** commands are separate for clarity. However, the options and behavior for the **clear authentication console** command are the same as in previous releases.*

Examples — The following command clears authentication for administrator Regina:

```
WX4400# clear authentication console Regina
success: change accepted.
```

See Also

- **clear authentication admin** on page 214
- **display aaa** on page 229
- **clear authentication dot1x** on page 216
- **clear authentication mac** on page 217

- **clear authentication mac** on page 217
- **clear authentication proxy** on page 218
- **set authentication console** on page 241

clear authentication dot1x

Removes an 802.1X authentication rule.

Syntax — `clear authentication dot1x {ssid ssid-name | wired} user-glob`

- **ssid *ssid-name*** — SSID name to which this authentication rule applies.
- **wired** — Clears a rule used for access over a WX wired-authentication port.
- ***user-glob*** — A single user or a set of users with 802.1X network access.

Specify a username, use the double-asterisk wildcard character (******) to specify all usernames, or use the single-asterisk wildcard character (*****) to specify a set of usernames up to or following the first delimiter character, either an *at* sign (**@**) or a period (**.**). (For details, see “User Globs” on page 30.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes 802.1X authentication for network users with usernames ending in *@thiscorp.com* who try to access SSID *finance*:

```
WX4400# clear authentication dot1x ssid finance
*@thiscorp.com
```

See Also

- **clear authentication admin** on page 214
- **clear authentication console** on page 215
- **clear authentication mac** on page 217
- **clear authentication mac** on page 217

- **clear authentication proxy** on page 218
- **display aaa** on page 229
- **set authentication dot1x** on page 243

clear authentication mac

Removes a MAC authentication rule.

Syntax — `clear authentication mac {ssid ssid-name | wired} mac-addr-glob`

- **ssid *ssid-name*** — SSID name to apply the authentication.
- **wired** — Clears a rule used for access over a WX wired-authentication port.
- ***mac-addr-glob*** — A single user or set of users with access via a MAC address. Specify a MAC address, or use the wildcard (*) character to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 31.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes a MAC authentication rule for access to SSID *thatcorp* by MAC addresses beginning with *aa:bb:cc*:

```
WX4400# clear authentication mac ssid thatcorp aa:bb:cc:*
```

See Also

- **clear authentication admin** on page 214
- **clear authentication console** on page 215
- **clear authentication dot1x** on page 216
- **clear authentication mac** on page 217
- **clear authentication proxy** on page 218
- **display aaa** on page 229
- **set authentication mac** on page 247

clear authentication proxy

Removes a proxy rule for third-party AP users.

Syntax — `clear authentication proxy ssid ssid-name user-glob`

- **ssid** *ssid-name* — SSID name to which this authentication rule applies.
- *user-glob* — User-glob associated with the rule you are removing.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command removes the proxy rule for SSID *mycorp* and userglob ****:

```
WX4400# clear authentication proxy ssid mycorp
```

See Also

- **set authentication proxy** on page 253
- **display aaa** on page 229

clear authentication web

Removes a WebAAA rule.

Syntax — `clear authentication web {ssid ssid-name | wired} user-glob`

- **ssid** *ssid-name* — SSID name to which this authentication rule applies.
- **wired** — Clears a rule used for access over a WX switch's wired-authentication port.
- *user-glob* — User-glob associated with the rule you are removing.

Defaults — None.

Access — Enabled.

History — Introduced in MSS 3.0.

Examples — The following command removes WebAAA for SSID *research* and userglob *temp*@thiscorp.com*:

```
WX4400# clear authentication web ssid research
temp*@thiscorp.com
```

See Also

- **clear authentication admin** on page 214
- **clear authentication console** on page 215
- **clear authentication dot1x** on page 216
- **clear authentication mac** on page 217
- **clear authentication mac** on page 217
- **set authentication web** on page 254
- **display aaa** on page 229

clear location policy Removes a rule from the location policy on a WX switch.

Syntax — `clear location policy rule-number`

- *rule-number* — Index number of a location policy rule to remove from the location policy.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To determine the index numbers of location policy rules, use the **display location policy** command. Removing all the ACEs from the location policy disables this function on the WX switch.

Examples — The following command removes location policy rule 4 from an WX switch's location policy:

```
WX4400# clear location policy 4
success: clause 4 is removed.
```

See Also

- **display location policy** on page 234
- **set location policy** on page 256

clear mac-user

Removes a user profile from the local database on the WX for a user authenticated by a MAC address.

(To remove a user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax — `clear mac-user mac-addr`

- *mac-addr* — MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Deleting a MAC user's profile from the database deletes the assignment of any attributes in the profile to the user.

Examples — The following command removes the user profile for a user at MAC address 01:02:03:04:05:06:

```
WX4400# clear mac-user 01:02:03:04:05:06
success: change accepted.
```

See Also

- **display aaa** on page 229
- **set mac-usergroup attr** on page 267
- **set mac-user attr** on page 261

clear mac-user attr Removes an authorization attribute from the user profile in the local database on the WX switch, for a user who is authenticated by a MAC address.

(To remove an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

Syntax — `clear mac-user mac-addr attr attribute-name`

- *mac-addr* — MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.
- *attribute-name* — Name of an attribute used to authorize the MAC user for a particular service or session characteristic. (For a list of authorization attributes, see Table 44 on page 262.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes an access control list (ACL) from the profile of a user at MAC address 01:02:03:04:05:06:

```
WX4400# clear mac-user 01:02:03:04:05:06 attr filter-id
success: change accepted.
```

See Also

- **display aaa** on page 229
- **set mac-user attr** on page 261

clear mac-user group

Removes a user group from the local database on the WX for a group of users authenticating with a MAC address.

(To remove a MAC user group profile in RADIUS, see the documentation for your RADIUS server.)

Syntax — `clear mac-user mac-addr group`

- *mac-addr* — MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Removing a MAC user from a MAC user group removes the group name from the user’s profile, but does not delete the user group from the local WX database. To remove the group, use **clear mac-usergroup**.

Examples — The following command deletes the user profile for a user at MAC address 01:02:03:04:05:06 from its user group:

```
WX4400# clear mac-user 01:02:03:04:05:06 group
success: change accepted.
```

See Also

- **clear mac-usergroup** on page 222
- **display aaa** on page 229
- **set mac-user** on page 260

clear mac-usergroup

Removes a user group from the local database on the WX for a group of users authenticating with a MAC address.

(To delete a MAC user group in RADIUS, see the documentation for your RADIUS server.)

Syntax — **clear mac-usergroup** *group-name*

- *group-name* — Name of an existing MAC user group.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — To remove a user from a MAC user group, use the **clear mac-user group** command.

Examples — The following command deletes the MAC user group *eastcoasters* from the local database:

```
WX4400# clear mac-usergroup eastcoasters
success: change accepted.
```

See Also

- **clear mac-usergroup attr** on page 223
- **display aaa** on page 229
- **set mac-usergroup attr** on page 267

**clear
mac-usergroup attr**

Removes an authorization attribute from a MAC user group in the local database on the WX, for a group of users who are authenticated by a MAC address.

(To unconfigure an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

Syntax — `clear mac-usergroup group-name attr attribute-name`

- *group-name* — Name of an existing MAC user group.
- *attribute-name* — Name of an attribute used to authorize the MAC users in the user group for a particular service or session characteristic. (For a list of authorization attributes, see Table 44 on page 262.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To remove the group itself, use the **clear mac-usergroup** command.

Examples — The following command removes the members of the MAC user group *eastcoasters* from a VLAN assignment by deleting the VLAN-Name attribute from the group:

```
WX4400# clear mac-usergroup eastcoasters attr vlan-name
success: change accepted.
```

See Also

- **clear mac-usergroup** on page 222
- **display aaa** on page 229
- **set mac-usergroup attr** on page 267

**clear
mobility-profile**

Removes a Mobility Profile entirely.

Syntax — `clear mobility-profile name`

- *name* — Name of an existing Mobility Profile.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes the Mobility Profile for user Nin:

```
WX1200# clear mobility-profile Nin
success: change accepted.
```

See Also

- **set mobility-profile** on page 269
- **set mobility-profile mode** on page 271
- **display mobility-profile** on page 235

clear user

Removes a user profile from the local database on the WX, for a user with a password.

(To remove a user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax — `clear user username`

- *username* — Username of a user with a password.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Deleting the user profile from the database deletes the assignment of any profile attributes to the user.

Examples — The following command deletes the user profile for user Nin:

```
WX4400# clear user Nin
success: change accepted.
```

See Also

- **display aaa** on page 229
- **set user** on page 271

clear user attr

Removes an authorization attribute from the user profile in the local database on the WX for a user with a password.

(To remove an authorization attribute from a RADIUS user profile, see the documentation for your RADIUS server.)

Syntax — `clear user username attr attribute-name`

- *username* — Username of a user with a password.
- *attribute-name* — Name of an attribute used to authorize the user for a particular service or session characteristic. (For a list of authorization attributes, see Table 44 on page 262.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes the Session-Timeout attribute from Hosni's user profile:

```
WX4400# clear user Hosni attr session-timeout
success: change accepted.
```

See Also

- **display aaa** on page 229
- **set user attr** on page 273

clear user group

Removes a user with a password from membership in a user group in the local database on the WX.

(To remove a user from a user group in RADIUS, see the documentation for your RADIUS server.)

Syntax — `clear user username group`

- *username* — Username of a user with a password.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Removing the user from the group removes the group name from the user profile, but does not delete either the user or the user group from the local WX database. To remove the group, use **clear usergroup**.

Examples — The following command removes the user Nin from a user group:

```
WX4400# clear user Nin group
success: change accepted.
```

See Also

- **clear usergroup** on page 227
- **display aaa** on page 229
- **set user group** on page 275

clear user logout

Restores access to a user who has been locked out of the system due to an expired password or exceeding the maximum number of failed login attempts.

Syntax — `clear user username logout`

Defaults — None.

Access — Enabled.

History — Introduced in MSS 6.0.

Usage — If a user's password has expired, or the user is unable to log in within the configured limit for login attempts, then the user is locked out of the system, and cannot gain access without the intervention of an administrator. Use this command to restore access to the user.

Examples — The following command restores access to user Nin, who had previously been locked out of the system:

```
WX# clear user Nin lockout
success: change accepted.
```

See Also

- **set user attr** on page 273
- **display aaa** on page 229

clear usergroup

Removes a user group and its attributes from the local database on the WX, for users with passwords.

(To delete a user group in RADIUS, see the documentation for your RADIUS server.)

Syntax — `clear usergroup group-name`

- *group-name* — Name of an existing user group.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Removing a user group from the local WX database does not remove the user profiles of the group members from the database.

Examples — The following command deletes the *cardiology* user group from the local database:

```
WX4400# clear usergroup cardiology
success: change accepted.
```

See Also

- **clear usergroup attr** on page 228
- **display aaa** on page 229
- **set usergroup** on page 275

clear usergroup attr

Removes an authorization attribute from a user group in the local database on the WX.

(To remove an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

Syntax — `clear usergroup group-name attr attribute-name`

- *group-name* — Name of an existing user group.
- *attribute-name* — Name of an attribute used to authorize all the users in the group for a particular service or session characteristic. (For a list of authorization attributes, see Table 44 on page 262.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes the members of the user group *cardiology* from a network access time restriction by deleting the Time-Of-Day attribute from the group:

```
WX4400# clear usergroup cardiology attr time-of-day
success: change accepted.
```

See Also

- **clear usergroup** on page 227
- **display aaa** on page 229
- **set usergroup** on page 275

display aaa Displays all current AAA settings.

Syntax — `display aaa`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. Web Portal section added, to indicate the state of the WebAAA feature in MSS Version 4.0.

Examples — To display all current AAA settings, type the following command:

```
WX4400# display aaa
Default Values
authport=1812 acctport=1813 timeout=5 acct-timeout=5
retrans=3 deadtime=0 key=(null) author-pass=(null)
Radius Servers
Server                Addr                Ports    T/o  Tries  Dead  State
-----
rs-3                  198.162.1.1        1821 1813  5    3    0    UP
rs-4                  198.168.1.2        1821 1813  77   11   2    UP
rs-5                  198.162.1.3        1821 1813  42   23   0    UP
Server groups
sg1: rs-3
sg2: rs-4
sg3: rs-5

Web Portal:
enabled

set authentication admin Jose sg3
set authentication console * none
set authentication mac ssid mycorp * local
set authentication dotlx ssid mycorp Geetha eap-tls
set authentication dotlx ssid mycorp * peap-mschapv2 sg1 sg2 sg3
set authentication dotlx ssid any ** peap-mschapv2 sg1 sg2 sg3
set accounting dotlx Nin ssid mycorp stop-only sg2
set accounting admin Natasha start-stop local

user Nin
Password = 082c6c64060b (encrypted)
Filter-Id = acl-999.in
Filter-Id = acl-999.out
```

```

user last-resort-guestssid
Vlan-Name = k2
user last-resort-any
Vlan-Name = foo
mac-user 01:02:03:04:05:06
usergroup eastcoasters
  session-timeout = 99

```

Table 42 describes the fields that can appear in **display aaa** output.

Table 42 display aaa Output

Field	Description
Default Values	RADIUS default values for all parameters.
authport	UDP port on the WX for transmission of RADIUS authorization and authentication messages. The default port is 1812.
acctport	UDP port on the WX for transmission of RADIUS accounting records. The default is port 1813.
timeout	Number of seconds the WX switch waits for a RADIUS server to respond before retransmitting. The default is 5 seconds.
acct-timeout	Number of seconds the WX waits for a RADIUS server to respond to an accounting request before retransmitting. The default is 5 seconds.
retrans	Number of times the WX switch retransmits a message before determining a RADIUS server unresponsive. The default is 3 times.
deadtime	Number of minutes the WX switch waits after determining a RADIUS server is unresponsive before trying to reconnect with this server. During the dead time, the RADIUS server is ignored by the WX. The default is 0 minutes.
key	Shared secret key, or password, used to authenticate to a RADIUS server. The default is no key.
author-pass	Password used for authorization to a RADIUS server for MAC authentication. The client MAC address is sent as the username and the author-pass string is sent as the password.
Radius Servers	Information about active RADIUS servers.
Server	Name of each RADIUS server currently active.
Addr	IP address of each RADIUS server currently active.
Ports	UDP ports that the WX switch uses for authentication messages and for accounting records.

Table 42 display aaa Output (continued)

T/o	Setting of timeouts on each RADIUS server currently active.
Tries	Number of retransmissions configured for each RADIUS server currently active. The default is 3 times.
Dead	Length of time until the server is considered responsive again.
State	Current state of each RADIUS server currently active: <ul style="list-style-type: none"> ■ UP (operating) ■ DOWN (unavailable)
Server groups	Names of RADIUS server groups and member servers configured on the WX switch.
Web Portal	State of the WebAAA feature: <ul style="list-style-type: none"> ■ enabled ■ disabled
set commands	List of commands used to configure AAA on the WX switch.
user and user group profiles	List of user and user group profiles stored in the local database on the WX switch.

See Also

- **set accounting {admin | console}** on page 235
- **set authentication admin** on page 239
- **set authentication console** on page 241
- **set authentication dot1x** on page 243
- **set authentication mac** on page 247
- **set authentication mac** on page 247
- **set authentication web** on page 254

display accounting statistics

Displays the AAA accounting records for wireless users. The records are stored in the local database on the WX.

(To display RADIUS accounting records, see the documentation for your RADIUS server.)

Syntax — `display accounting statistics`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. Formatting of output enhanced for readability in Version 4.2

Examples — To display the locally stored accounting records, type the following command:

```
WX4400# display accounting statistics
Dec 14 00:39:48
Acct-Status-Type=STOP
Acct-Authentic=0
Acct-Multi-Session-Id=SESS-3-01f82f-520236-24bb1223
Acct-Session-Id=SESS-3-01f82f-520236-24bb1223
User-Name=vineet
AAA_ACCT_SVC_ATTR=2
Acct-Session-Time=551
Event-Timestamp=1134520788
Acct-Output-Octets=3204
Acct-Input-Octets=1691
Acct-Output-Packets=20
Acct-Input-Packets=19
AAA_VLAN_NAME_ATTR=default
Calling-Station-Id=00-06-25-12-06-38
Nas-Port-Id=3/1
Called-Station-Id=00-0B-0E-00-CC-01
AAA_SSID_ATTR=vineet-dot1x

Dec 14 00:39:53
Acct-Status-Type=START
Acct-Authentic=0
User-Name=vineet
Acct-Multi-Session-Id=SESS-4-01f82f-520793-bd779517
Acct-Session-Id=SESS-4-01f82f-520793-bd779517
Event-Timestamp=1134520793
```



```

AAA_ACCT_SVC_ATTR=2
AAA_VLAN_NAME_ATTR=default
Calling-Station-Id=00-06-25-12-06-38
Nas-Port-Id=3/1
Called-Station-Id=00-0B-0E-00-CC-01
AAA_SSID_ATTR=vineet-dot1x

```

Table 43 describes the fields that can appear in **display accounting statistics** output.

Table 43 display accounting statistics Output

Field	Description
Date and time	Date and time of the accounting record.
Acct-Status-Type	Type of accounting record: <ul style="list-style-type: none"> ▪ START ▪ STOP ▪ UPDATE
Acct-Authentic	Location where the user was authenticated (if authentication took place) for the session: <ul style="list-style-type: none"> ▪ 1 — RADIUS server ▪ 2 — Local WX database
User-Name	Username of a user with a password.
Acct-Multi-Session-Id	Unique accounting ID for multiple related sessions in a log file.
AAA_TTY_ATTR	For sessions conducted through a console or administrative Telnet connection, the Telnet terminal number.
Event-Timestamp	Time (in seconds since January 1, 1970) at which the event was triggered. (See RFC 2869 for more information.)
Acct-Session-Time	Number of seconds that the session has been online.
Acct-Output-Octets	Number of octets the WX has sent during the session.
Acct-Input-Octets	Number of octets the WX has received during the session.
Acct-Output-Packets	Number of packets the WX has sent during the session.
Acct-Input-Packets	Number of packets the WX has received during the session.
Vlan-Name	Name of the client VLAN.
Calling-Station-Id	MAC address of the supplicant (client).

Table 43 display accounting statistics Output (continued)

Nas-Port-Id	Number of the port and radio on the MAP through which the session was conducted.
Called-Station-Id	MAC address of the MAP through which the client reached the network.

See Also

- **clear accounting** on page 213
- **display aaa** on page 229
- **set accounting {admin | console}** on page 235

display location policy

Displays the list of location policy rules that make up the location policy on an WX switch.

Syntax — `display location policy`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command displays the list of location policy rules in the location policy on an WX switch:

```
WX4400 display location policy
```

Id Clauses

```
-----
1) deny if user eq *.theirfirm.com
2) permit vlan guest_1 if vlan neq *.wodefirm.com
3) permit vlan bld4.tac inacl tac_24.in if user eq *.ny.wodefirm.com
```

See Also

- **clear location policy** on page 219
- **set location policy** on page 256

display mobility-profile

Displays the named Mobility Profile. If you do not specify a Mobility Profile name, this command shows all Mobility Profile names and port lists on the WX.

Syntax — `display mobility-profile [name]`

- *name* — Name of an existing Mobility Profile.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command displays the Mobility Profile *magnolia*:

```
WX1200# display mobility-profile magnolia
Mobility Profiles
Name                Ports
=====
magnolia            AP 2
```

See Also

- **clear mobility-profile** on page 224
- **set mobility-profile** on page 269

set accounting {admin | console}

Sets up accounting services for specified wireless users with administrative access, and defines the accounting records and where they are sent.

Syntax — `set accounting {admin | console} {user-glob} {start-stop | stop-only} method1 [method2] [method3] [method4]`

- **admin** — Users with administrative access to the WX switch through Telnet or Web View.
- **console** — Users with administrative access to the WX switch through a console connection.
- *user-glob* — Single user or set of users with administrative access or network access.

- Specify a username, use the double-asterisk wildcard character (******) to specify all usernames, or use the single-asterisk wildcard character (*****) to specify a set of usernames up to or following the first delimiter character—either an at sign (**@**) or a period (**.**). (For details, see “User Globs” on page 30.)



*This option does not apply if **mac** is specified. For **mac**, specify a **mac-addr-glob**. (See “MAC Address Globs” on page 31.)*

- **start-stop** — Sends accounting records at the start and end of a network session.
- **stop-only** — Sends accounting records only at the end of a network session.
- *method1, method2, method3, method4* — At least one of up to four methods that MSS uses to process accounting records. Specify one or more of the following methods in priority order. If the first method does not succeed, MSS tries the second method, and so on.

A method can be one of the following:

- **local** — Stores accounting records in the local database on the WX switch. When the local accounting storage space is full, MSS overwrites older records with new ones.
- *server-group-name* — Stores accounting records on one or more Remote Authentication Dial-In User Service (RADIUS) servers. You can also enter the names of existing RADIUS server groups as methods.

Defaults — Accounting is disabled for all users by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — For network users with start-stop accounting whose records are sent to a RADIUS server, MSS sends interim updates to the RADIUS server when the user roams.

Examples — The following command issues start-and-stop accounting records at the local WX database for administrator Natasha, when she accesses the switch using Telnet or Web Manager:

```
WX4400# set accounting admin Natasha start-stop local
success: change accepted.
```

See Also

- **clear accounting** on page 213
- **display accounting statistics** on page 232

set accounting {dot1x | mac | web | last-resort}

Sets up accounting services for specified wireless users with network access, and defines the accounting records and where they are sent.

Syntax — `set accounting {dot1x | mac | web | last-resort} {ssid ssid-name | wired} {user-glob | mac-addr-glob} {start-stop | stop-only} method1 [method2] [method3] [method4]`

- **dot1x** — Users with network access through the WX switch who are authenticated by 802.1X.
- **mac** — Users with network access through the WX switch who are authenticated by MAC authentication
- **web** — Users with network access through the WX switch who are authenticated by WebAAA
- **ssid ssid-name** — SSID name to which this accounting rule applies. To apply the rule to all SSIDs, type any.
- **wired** — Applies this accounting rule specifically to users who are authenticated on a wired authentication port.
- **user-glob** — Single user or set of users with administrative access or network access.

Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character — either an *at* sign (@) or a period (.). (For details, see “User Globs” on page 30.)



*This option does not apply if **mac** or **last-resort** is specified. For **mac**, specify a **mac-addr-glob**. (See “MAC Address Globs” on page 31.)*

- **mac-addr-glob** — A single user or set of users with access via a MAC address. Specify a MAC address, or use the wildcard (*) character to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 31.)

This option applies only when **mac** is specified.

- **start-stop** — Sends accounting records at the start and end of a network session.
- **stop-only** — Sends accounting records only at the end of a network session.
- *method1, method2, method3, method4* — At least one of up to four methods that MSS uses to process accounting records. Specify one or more of the following methods in priority order. If the first method does not succeed, MSS tries the second method, and so on.

A method can be one of the following:

- **local** — Stores accounting records in the local database on the WX switch. When the local accounting storage space is full, MSS overwrites older records with new ones.
- *server-group-name* — Stores accounting records on one or more Remote Authentication Dial-In User Service (RADIUS) servers. You can also enter the names of existing RADIUS server groups as methods.

Defaults — Accounting is disabled for all users by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — For network users with start-stop accounting profiles whose records are sent to a RADIUS server, MSS sends interim updates to the RADIUS server when the user roams.

Examples — The following command issues stop-only records to the RADIUS server group *sg2* for network user *Nin*, who is authenticated by 802.1X:

```
WX4400# set accounting dot1x Nin stop-only sg2
success: change accepted.
```

See Also

- **clear accounting** on page 213
- **display accounting statistics** on page 232

set authentication admin

Configures authentication and defines where it is performed for specified users with administrative access through Telnet or Web Manager.

Syntax — set authentication admin

```
user-glob method1 [method2] [method3] [method4]
```

- *user-glob* — Single user or set of users with administrative access over the network through Telnet or Web Manager.

Specify a username, use the double-asterisk wildcard character (******) to specify all usernames, or use the single-asterisk wildcard character (*****) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (**@**) or a period (**.**). (For details, see “User Globs” on page 30.)

- *method1, method2, method3, method4* — At least one of up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

A method can be one of the following:

- **local** — Uses the local database of usernames and user groups on the WX switch for authentication.
- *server-group-name* — Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.
- **none** — *For users with administrative access only*, MSS performs no authentication, but prompts for a username and password and accepts any combination of entries, including blanks.



*The authentication method **none** you can specify for administrative access is different from the fallthru authentication type **none**, which applies only to network access. The authentication method **none** allows access to the WX switch by an administrator. The fallthru authentication type **none** denies access to a network user. (See “set service-profile auth-fallthru” on page 434.)*

For more information, see “Usage.”

Defaults — By default, authentication is deactivated for all admin users. The default authentication method in an admin authentication rule is **local**. MSS checks the local WX database for authentication.

Access — Enabled.

History —Introduced in MSS Version 3.0.



*The syntax descriptions for the **set authentication** commands are separated for clarity. However, the options and behavior for the **set authentication admin** command are the same as in previous releases.*

Usage — You can configure different authentication methods for different groups of users. (For details, see “User Globs, MAC Address Globs, and VLAN Globs” on page 30.)

If you specify multiple authentication methods in the **set authentication console** command, MSS applies them in the order that they appear in the command, with these results:

If the first method responds with pass or fail, the evaluation is final.

If the first method does not respond, MSS tries the second method, and so on.

However, if **local** appears first, followed by a RADIUS server group, MSS ignores any failed searches in the local WX database and sends an authentication request to the RADIUS server group.



If a AAA rule specifies local as a secondary AAA method, to be used if the RADIUS servers are unavailable, and MSS authenticates a client with the local method, MSS starts again at the beginning of the method list when attempting to authorize the client. This can cause unexpected delays during client processing and can cause the client to time out before completing logon.

Examples — The following command configures administrator Jose, who connects via Telnet, for authentication on RADIUS server group sg3:

```
WX4400# set authentication admin Jose sg3
success: change accepted.
```

See Also

- **clear authentication admin** on page 214
- **display aaa** on page 229
- **set authentication console** on page 241
- **set authentication dot1x** on page 243
- **set authentication mac** on page 247

- **set authentication mac** on page 247
- **set authentication web** on page 254

set authentication console

Configures authentication and defines where it is performed for specified users with administrative access through a console connection.

Syntax — set authentication console

```
user-glob method1 [method2] [method3] [method4]
```

- *user-glob* — Single user or set of users with administrative access through the switch's console.

Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see “User Globs” on page 30.)

- *method1, method2, method3, method4* — At least one of up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

A method can be one of the following:

- **local** — Uses the local database of usernames and user groups on the WX switch for authentication.
- *server-group-name* — Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.
- **none** — *For users with administrative access only*, MSS performs no authentication, but prompts for a username and password and accepts any combination of entries, including blanks.



The authentication method **none** you can specify for administrative access is different from the fallthru authentication type **none**, which applies only to network access. The authentication method **none** allows access to the WX switch by an administrator. The fallthru authentication type **none** denies access to a network user. (See “set service-profile auth-fallthru” on page 434.)

Defaults — By default, authentication is deactivated for all console users, and the default authentication method in a console authentication rule is **none**. MSS requires no username or password, by default. These users can press Enter at the prompts for administrative access.



It is recommended that you change the default setting unless the WX is in a secure physical location.

Access — Enabled.

History — Introduced in MSS Version 3.0.



*The syntax description for the **set authentication** commands are separated for clarity. However, the options and behavior for the **set authentication console** command are the same as in previous releases.*

Usage — You can configure different authentication methods for different groups of users. (For details, see “User Globs, MAC Address Globs, and VLAN Globs” on page 30.)

If you specify multiple authentication methods in the **set authentication console** command, MSS applies them in the order in which they appear in the command, with these results:

If the first method responds with pass or fail, the evaluation is final.

If the first method does not respond, MSS tries the second method, and so on.

However, if **local** appears first, followed by a RADIUS server group, MSS ignores any failed searches in the local WX database and sends an authentication request to the RADIUS server group.

Examples — To set the console port so that it does *not* enforce username-password authentication for administrators, type the following command:

```
WX4400# set authentication console * none
success: change accepted.
```

See Also

- **clear authentication console** on page 215
- **display aaa** on page 229

- **set authentication admin** on page 239
- **set authentication dot1x** on page 243
- **set authentication mac** on page 247
- **set authentication mac** on page 247
- **set authentication web** on page 254

set authentication dot1x

Configures authentication and defines how it is performed for specified wireless or wired authentication clients who use an IEEE 802.1X authentication protocol to access the network through the WX.

Syntax — **set authentication dot1x** {**ssid** *ssid-name* | **wired**} *user-glob* [**bonded**] *protocol method1* [*method2*] [*method3*] [*method4*]

- **ssid** *ssid-name* — SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type **any**.
- **wired** — Applies this authentication rule specifically to users connected to a wired authentication port.
- *user-glob* — A single user or a set of users with 802.1X network access.

Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character — either an *at* sign (@) or a period (.). (For details, see “User Globs” on page 30.)

- **bonded** — Enables Bonded Auth™ (bonded authentication). When this feature is enabled, MSS authenticates the user only if the computer the user is on has already been authenticated.
- *protocol* — Protocol used for authentication. Specify one of the following:
 - **eap-md5** — Extensible Authentication Protocol (EAP) with message-digest algorithm 5. *For wired authentication clients:*
 Uses challenge-response to compare hashes
 Provides *no* encryption or integrity checking for the connection
 - **eap-tls** — EAP with Transport Layer Security (TLS):

Provides mutual authentication, integrity-protected negotiation, and key exchange

Requires X.509 public key certificates on both sides of the connection

Provides encryption and integrity checking for the connection

Cannot be used with RADIUS server authentication (requires user information to be in the WX local database)

- **peap-mschapv2** — Protected EAP (PEAP) with Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP-V2). *For wireless clients:*

Uses TLS for encryption and data integrity checking and server-side authentication.

Provides MS-CHAP-V2 mutual authentication.

Only the server side of the connection needs a certificate.

The wireless client authenticates using TLS to set up an encrypted session. Then MS-CHAP-V2 performs mutual authentication using the specified AAA method.

- **pass-through** — MSS sends all the EAP protocol processing to a RADIUS server.



EAP-MD5 does not work with Microsoft wired authentication clients.

- *method1, method2, method3, method4* — At least one and up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

A method can be one of the following:

- **local** — Uses the local database of usernames and user groups on the WX switch for authentication.
- *server-group-name* — Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.

RADIUS servers cannot be used with the EAP-TLS protocol.

Defaults — By default, authentication is unconfigured for all clients with network access through MAP ports or wired authentication ports on the WX switch. Connection, authorization, and accounting are also disabled for these users.

Bonded authentication is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You can configure different authentication methods for different groups of users by “globbing.” (For details, see “User Globs” on page 30.)

You can configure a rule either for wireless access to an SSID, or for wired access through a WX wired authentication port. If the rule is for wireless access to an SSID, specify the SSID name or specify **any** to match on all SSID names. If the rule is for wired access, specify **wired** instead of an SSID name.

You cannot configure client authentication that uses both EAP-TLS protocol and one or more RADIUS servers. EAP-TLS authentication is supported only on the local WX database.

If you specify multiple authentication methods in the **set authentication dot1x** command, MSS applies them in the order in which they appear in the command, with these results:

If the first method responds with pass or fail, the evaluation is final.

If the first method does not respond, MSS tries the second method, and so on.

However, if **local** appears first, followed by a RADIUS server group, MSS overrides any failed searches in the local WX database and sends an authentication request to the server group.

If the user does not support 802.1X, MSS attempts to perform MAC authentication for the user. In this case, if the WX configuration contains a **set authentication mac** command that matches the SSID the user is attempting to access and the user MAC address, MSS uses the method specified by the command. Otherwise, MSS uses local MAC authentication by default.

If the username does not match an authentication rule for the SSID the user is attempting to access, MSS uses the *fallthru* authentication type configured for the SSID, which can be **last-resort**, **web-portal** (for WebAAA), or **none**.

Examples — The following command configures EAP-TLS authentication in the local WX database for SSID *mycorp* and 802.1X client Geetha:

```
WX4400# set authentication dot1x ssid mycorp Geetha eap-tls
local
success: change accepted.
```

The following command configures PEAP-MS-CHAP-V2 authentication at RADIUS server groups *sg1* through *sg3* for all 802.1X clients at *example.com* who want to access SSID *examplecorp*:

```
WX4400# set authentication dot1x ssid examplecorp
*@example.com peap-mschapv2 sg1 sg2 sg3
success: change accepted.
```

See Also

- **clear authentication dot1x** on page 216
- **display aaa** on page 229
- **set authentication admin** on page 239
- **set authentication console** on page 241
- **set authentication mac** on page 247
- **set authentication mac** on page 247
- **set authentication web** on page 254
- **set service-profile auth-fallthru** on page 434

set authentication mac

Configures authentication and defines where it is performed for specified non-802.1X users with network access through a media access control (MAC) address.

Syntax — set authentication mac

```
{ssid ssid-name | wired} mac-addr-glob method1
[method2] [method3] [method4]
```

- **ssid** *ssid-name* — SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type **any**.
- **wired** — Applies this authentication rule specifically to users connected to a wired authentication port.
- *mac-addr-glob* — A single user or set of users with access via a MAC address. Specify a MAC address, or use the wildcard (*) character to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 31.)
- *method1*, *method2*, *method3*, *method4* — At least one of up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

A method can be one of the following:

- **local** — Uses the local database of usernames and user groups on the WX switch for authentication.
- *server-group-name* — Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.

For more information, see “Usage.”

Defaults — By default, authentication is deactivated for all MAC users, which means MAC address authentication fails by default. When using RADIUS for authentication, the default password for a MAC user is the MAC address of the user.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You can configure different authentication methods for different groups of MAC addresses by “globbing.” (For details, see “User Globs, MAC Address Globs, and VLAN Globs” on page 30.)

If you specify multiple authentication methods in the **set authentication mac** command, MSS applies them in the order in which they appear in the command, with these results:

If the first method responds with pass or fail, the evaluation is final.

If the first method does not respond, MSS tries the second method, and so on.

However, if **local** appears first, followed by a RADIUS server group, MSS ignores any failed searches in the local WX database and sends an authentication request to the RADIUS server group.

If the WX configuration contains a **set authentication mac** command that matches the SSID the user is attempting to access and the user MAC address, MSS uses the method specified by the command. Otherwise, MSS uses local MAC authentication by default.

If the username does not match an authentication rule for the SSID the user is attempting to access, MSS uses the *fallthru* authentication type configured for the SSID, which can be **last-resort**, **web** (for WebAAA), or **none**.

Examples — To use the local WX database to authenticate all users who access the *mycorp2* SSID by their MAC address, type the following command:

```
WX4400# set authentication ssid mycorp2 mac ** local
success: change accepted.
```

See Also

- **clear authentication mac** on page 217
- **display aaa** on page 229
- **set authentication admin** on page 239
- **set authentication console** on page 241
- **set authentication dot1x** on page 243
- **set authentication mac** on page 247
- **set authentication web** on page 254

set authentication max-attempts

Specifies the maximum number of login attempts users can make before being locked out of the system.

Syntax — `set authentication max-attempts number`

Defaults — For Telnet or SSH sessions, a maximum of 4 failed login attempts are allowed by default. For console or network sessions, an unlimited number of failed login attempts are allowed by default.

- *number* — Number of allowable login attempts for a user. You can specify a number between 0 – 2147483647. Specifying 0 causes the number of allowable login attempts to reset to the default values.

Access — Enabled.

History — Introduced in MSS 6.0.

Usage — Use this command to specify the maximum number of failed login attempts allowed for a user. If the user is unable to log in within the specified number of attempts, he or she is locked out of the system, and the user's access must be manually restored with the **clear user lockout** command.

Examples — To allow users a maximum of 3 attempts to log into the system, type the following command:

```
WX# set authentication max-attempts 3
```

See Also

- **clear user lockout** on page 226
- **set authentication minimum-password-length** on page 251
- **set authentication password-restrict** on page 252

**set authentication
max-attempts**

Specifies the maximum number of login attempts users can make before being locked out of the system.

Syntax — `set authentication max-attempts number`

- *number* — Number of allowable login attempts for a user. You can specify a number between 0 – 2147483647. Specifying 0 causes the number of allowable login attempts to reset to the default values.

Defaults — For Telnet or SSH sessions, a maximum of 4 failed login attempts are allowed by default. For console or network sessions, an unlimited number of failed login attempts are allowed by default.

Access — Enabled.

History — Introduced in MSS 6.0.

Usage — Use this command to specify the maximum number of failed login attempts allowed for a user. If the user is unable to log in within the specified number of attempts, he or she is locked out of the system, and the user's access must be manually restored with the **clear user lockout** command.

Examples — To allow users a maximum of 3 attempts to log into the system, type the following command:

```
WX# set authentication max-attempts 3
success: change accepted.
```

See Also

- **clear user lockout** on page 226
- **set authentication minimum-password-length** on page 251
- **set authentication password-restrict** on page 252

**set authentication
minimum-password
-length**

Specifies the minimum allowable length for user passwords.

Syntax — `set authentication minimum-password-length length`

- *length* — Minimum number of characters that can be in a user password. You can specify a minimum password length between 0 – 32 characters. Specifying 0 removes the restriction on password length.

Defaults — By default, there is no minimum length for user passwords.

Access — Enabled.

History — Introduced in MSS 6.0.

Usage — Use this command to specify the minimum length for user passwords. When this command is configured, you cannot configure a password shorter than the specified length.

When you enable this command, MSS evaluates the passwords configured on the WX and displays a list of users whose password does not meet the minimum length restriction.

Examples — To set the minimum length for user passwords at 7 characters, type the following command:

```
WX# set authentication minimum-password-length 7
```

```
Warning: The following users have passwords that are shorter  
than the minimum password length:
```

```
dan  
admin  
user2  
goofball
```

```
success: change accepted.
```

See Also

- **clear user lockout** on page 226
- **set authentication minimum-password-length** on page 251
- **set user** on page 271

**set authentication
password-restrict**

Activates password restrictions for network and administrative users.

Syntax — `set authentication password-restrict {enable | disable}`

- **enable** — Enables password restrictions on the WX.
- **disable** — Disables password restrictions on the WX.

Defaults — By default the password restrictions are disabled.

Access — Enabled.

History — Introduced in MSS 6.0.

Usage — When this command is enabled, the following password restrictions take effect:

Passwords must be a minimum of 10 characters in length, and a mix of uppercase letters, lowercase letters, numbers, and special characters, including at least two of each (for example, *Tre%Pag32!*).

A user cannot reuse any of his or her 10 previous passwords (not applicable to network users).

When a user changes his or her password, at least 4 characters must be different from the previous password.

When you enable the password restrictions, MSS evaluates the passwords configured on the WX switch and displays a list of users whose password does not meet the restriction on length and character types.

Examples — To enable password restrictions on the WX switch, type the following command:

```
WX# set authentication password-restrict enable
warning: the following users have passwords that do not have
at least 2 each of upper-case letters, lower-case letters,
numbers and special characters -
  dan
  admin
  user1
  user2
  goofball
  dang
success: change accepted.
```

See Also

- **clear user lockout** on page 226
- **set authentication minimum-password-length** on page 251
- **set authentication max-attempts** on page 250

set authentication proxy

Configures a proxy authentication rule for a third-party AP's wireless users.

Syntax — `set authentication proxy ssid ssid-name user-glob radius-server-group`

- **ssid ssid-name** — SSID name to which this authentication rule applies.
- **user-glob** — A single user or a set of users. Specify a username, use the double-asterisk wildcard character (******) to specify all usernames, or use the single-asterisk wildcard character (*****) to specify a set of usernames up to or following the first delimiter character—either an at sign (**@**) or a period (**.**). (For details, see “User Globs, MAC Address Globs, and VLAN Globs” on page 30.)
- **radius-server-group** — A group of RADIUS servers used for authentication.

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.0.

Usage — AAA for third-party AP users has additional configuration requirements. See the “Configuring AAA for Users of Third-Party APs” section in the “Configuring AAA for Network Users” chapter of the [Wireless LAN Switch and Controller Configuration Guide](#).

Examples — The following command configures a proxy authentication rule that matches on all usernames associated with SSID *mycorp*. MSS uses RADIUS server group *svrgrp1* to proxy RADIUS requests and hence to authenticate and authorize the users.

```
WX4400# set authentication proxy ssid mycorp ** svrgrp1
```

See Also

- **clear authentication proxy** on page 218
- **set radius proxy client** on page 585
- **set radius proxy port** on page 586

set authentication web

Configures an authentication rule to allow a user to log in to the network using a web page served by the WX. The rule can be activated if the user is not otherwise granted or denied access by 802.1X, or granted access by MAC authentication.

Syntax — **set authentication web** {**ssid** *ssid-name* | **wired**}
user-glob *method1* [*method2*] [*method3*] [*method4*]

- *user-glob* — A single user or a set of users.
 Specify a username, use the double-asterisk wildcard character (******) to specify all usernames, or use the single-asterisk wildcard character (*****) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (**@**) or a period (**.**). (For details, see “User Globs” on page 30.)
- **ssid** *ssid-name* — SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type **any**.
- **wired** — Applies this authentication rule specifically to users connected to a wired authentication port.
- *method1*, *method2*, *method3*, *method4* — At least one and up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

A method can be one of the following:

- **local** — Uses the local database of usernames and user groups on the WX switch for authentication.
- *server-group-name* — Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.

RADIUS servers cannot be used with the EAP-TLS protocol.

For more information, see “Usage.”

Defaults — By default, authentication is unconfigured for all clients with network access through MAP ports or wired authentication ports on the WX switch. Connection, authorization, and accounting are also disabled for these users.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You can configure different authentication methods for different groups of users by “globbing.” (For details, see “User Globbs” on page 30.)

You can configure a rule either for wireless access to an SSID, or for wired access through a WX wired authentication port. If the rule is for wireless access to an SSID, specify the SSID name or specify **any** to match on all SSID names. If the rule is for wired access, specify **wired** instead of an SSID name.

If you specify multiple authentication methods in the **set authentication web** command, MSS applies them in the order in which they appear in the command, with these results:

If the first method responds with pass or fail, the evaluation is final.

If the first method does not respond, MSS tries the second method, and so on.

However, if **local** appears first, followed by a RADIUS server group, MSS overrides any failed searches in the local WX database and sends an authentication request to the server group.

MSS uses a WebAAA rule only under the following conditions:

The client is not denied access by 802.1X or does not support 802.1X.

The client MAC address does not match a MAC authentication rule.

The fallthru method is **web**. (For a wireless authentication rule, the fallthru method is specified by the **set service-profile auth-fallthru** command. For a wired authentication rule, the fallthru method is specified by the **auth-fall-thru** option of the **set port type wired-auth** command.)

Examples — The following command configures a WebAAA rule in the local WX database for SSID *ourcorp* and userglob *rnd**:

```
WX4400# set authentication web ssid ourcorp rnd* local
success: change accepted.
```

See Also

- **clear authentication proxy** on page 218
- **display aaa** on page 229
- **set authentication admin** on page 239
- **set authentication console** on page 241
- **set authentication dot1x** on page 243
- **set authentication mac** on page 247

set location policy

Creates and enables a location policy on a WX. The location policy enables you to locally set or change authorization attributes for a user after the user is authorized by AAA, without making changes to the AAA server.

Syntax — `set location policy deny if {ssid operator ssid-name | vlan operator vlan-glob | user operator user-glob | port port-list | ap ap-num} [before rule-number | modify rule-number]`

Syntax — `set location policy permit {vlan vlan-name | inacl inacl-name | outacl outacl-name} if {ssid operator ssid-name | vlan operator vlan-glob | user operator user-glob | port port-list | ap ap-num} [before rule-number | modify rule-number]`

- **deny** — Denies access to the network to users with attributes that match the location policy rule.
- **permit** — Allows access to the network or to a specified VLAN, and/or assigns a particular security ACL to users with attributes matching match the location policy rule.
- **Action options** — For a permit rule, MSS changes the attributes assigned to the user to the values specified by the following options:
 - **vlan** *vlan-name* — Name of an existing VLAN to assign to users with attributes matching the location policy rule.

- **inacl** *inacl-name* — Name of an existing security ACL to apply to packets sent to the WX with attributes matching the location policy rule.

Optionally, you can add the suffix **.in** to the name.

- **outacl** *outacl-name* — Name of an existing security ACL to apply to packets sent from the WX with attributes matching the location policy rule.

Optionally, you can add the suffix **.out** to the name.

- **Condition options** — MSS takes the action specified by the rule if all conditions in the rule are met. You can specify one or more of the following conditions:
- **ssid operator** *ssid-name* — SSID with which the user is associated. The *operator* must be **eq**, which applies the location policy rule to all users associated with the SSID. Asterisks (wildcards) are not supported in SSID names. You must specify the complete SSID name.
- **vlan operator** *vlan-glob* — VLAN-Name attribute assigned by AAA and condition that determines if the location policy rule applies. Replace *operator* with one of the following operands:

- **eq** — Applies the location policy rule to all users assigned VLAN names matching *vlan-glob*.
- **neq** — Applies the location policy rule to all users assigned VLAN names *not* matching *vlan-glob*.

For *vlan-glob*, specify a VLAN name, use the double-asterisk wildcard character (******) to specify all VLAN names, or use the single-asterisk wildcard character (*****) to specify a set of VLAN names up to or following the first delimiter character, either an *at* sign (**@**) or a period (**.**). (For details, see “VLAN Globs” on page 32.)

- **user operator** *user-glob* — Username and condition that determines if the location policy rule applies. Replace *operator* with one of the following operands:
- **eq** — Applies the location policy rule to all usernames matching *user-glob*.
- **neq** — Applies the location policy rule to all usernames *not* matching *user-glob*.

For *user-glob*, specify a username, use the double-asterisk wildcard character (******) to specify all usernames, or use the single-asterisk wildcard character (*****) to specify a set of usernames up to or following the first delimiter character, either an *at* sign (**@**) or a period (**.**). (For details, see “User Globs” on page 30.)

- **before** *rule-number* — Inserts the new location policy rule in front of another rule in the location policy. Specify the number of the existing location policy rule. (To determine the number, use the **display location policy** command.)
- **modify** *rule-number* — Replaces the rule in the location policy with the new rule. Specify the number of the existing location policy rule. (To determine the number, use the **display location policy** command.)
- **port** *port-list* — List of physical port(s) that determines if the location policy rule applies.

Defaults — By default, users are permitted VLAN access and assigned security ACLs according to the VLAN-Name and Filter-Id attributes applied to the users during normal authentication and authorization.

Access — Enabled.

History — Introduced in MSS Version 3.0. SSID option added in MSS Version 3.2.

Usage — Only a single location policy is allowed per WX switch. Once configured, the location policy becomes effective immediately. To disable location policy operation, use the **clear location policy** command.

Conditions within a rule are AND’ed. All conditions in the rule must match for MSS to take the specified action. If the location policy contains multiple rules, MSS compares the user information to the rules one at a time, in the order the rules appear in the WX configuration file, beginning with the rule at the top of the list. MSS continues comparing until a user matches all conditions in a rule or until there are no more rules.

The order of rules in the location policy is important to ensure users are properly granted or denied access. To position rules within the location policy, use **before rule-number** and **modify rule-number** in the **set location policy** command, and the **clear location policy rule-number** command.

When applying security ACLs:

Use **inac1** *inac1-name* to filter traffic that enters the WX from users via a MAP access port or wired authentication port, or from the network via a network port.

Use **outac1** *outac1-name* to filter traffic sent from the switch to users via a MAP access port or wired authentication port, or from the network via a network port.

You can optionally add the suffixes **.in** and **.out** to *inac1-name* and *outac1-name* so that they match the names of security ACLs stored in the local WX database.

Examples — The following command denies network access to all users at *.theirfirm.com, causing them to fail authorization:

```
WX4400# set location policy deny if user eq *.theirfirm.com
```

The following command authorizes access to the *guest_1* VLAN for all users who are not at *.wodefirm.com:

```
WX4400# set location policy permit vlan guest_1 if user neq *.wodefirm.com
```

The following command authorizes users at *.ny.ourfirm.com to access the *bld4.tac* VLAN instead, and applies the security ACL *tac_24* to the traffic they receive:

```
WX4400# set location policy permit vlan bld4.tac
outac1 tac_24 if user eq *.ny.ourfirm.com
```

The following command authorizes access to users on VLANs with names matching *bld4.** and applies security ACLs *svcs_2* to the traffic they send and *svcs_3* to the traffic they receive:

```
WX4400# set location policy permit inac1 svcs_2 outac1 svcs_3
if vlan eq bldg4.*
```

The following command authorizes users entering the network on WX ports 1 and 2 to use the *floor2* VLAN, overriding any settings from AAA:

```
WX4400# set location policy permit vlan floor2 if port 1-2
```

The following command places all users who are authorized for SSID *tempvendor_a* into VLAN *kiosk_1*:

```
WX1200# set location policy permit vlan kiosk_1 iff ssid eq
tempvendor_a
success: change accepted
```

See Also

- **clear location policy** on page 219
- **display location policy** on page 234

set mac-user

Configures a user profile in the local database on the WX for a user who can authenticate by a MAC address, and optionally adds the user to a MAC user group.

(To configure a MAC user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax — **set mac-user** *mac-addr* [**group** *group-name*]

- *mac-addr* — MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.
- *group-name* — Name of an existing MAC user group.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — MSS does not require MAC users to belong to user groups.

Users authenticated by MAC address are authenticated only for network access through the WX. MSS does not support passwords for MAC users.

Examples — The following command creates a user profile for a user at MAC address 01:02:03:04:05:06 and assigns the user to the *eastcoasters* user group:

```
WX4400# set mac-user 01:02:03:04:05:06 group eastcoasters
success: change accepted.
```

See Also

- **clear mac-user** on page 220
- **display aaa** on page 229

set mac-user attr

Assigns an authorization attribute in the local database on the WX to a user authenticating with a MAC address.

(To assign authorization attributes through RADIUS, see the documentation for your RADIUS server.)

Syntax — **set mac-user** *mac-addr* **attr** *attribute-name value*

- *mac-addr* — MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.
- *attribute-name value* — Name and value of an attribute used to authorize a MAC user for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to local users, see Table 44.

Table 44 Authentication Attributes for Local Users

Attribute	Description	Valid Value(s)
encryption-type	Type of encryption required for access by the client. Clients who attempt to use an unauthorized encryption method are rejected.	<p>One of the following numbers that identifies an encryption algorithm:</p> <ul style="list-style-type: none"> ▪ 1—AES_CCM (Advanced Encryption Standard using Counter with CBC-MAC) ▪ 2—Reserved ▪ 4—TKIP (Temporal Key Integrity Protocol) ▪ 8—WEP_104 (the default) (Wired-Equivalent Privacy protocol using 104 bits of key strength) ▪ 16—WEP_40 (Wired-Equivalent Privacy protocol using 40 bits of key strength) ▪ 32—NONE (no encryption) ▪ 64—Static WEP <p>In addition to these values, you can specify a sum of them for a combination of allowed encryption types. For example, to specify WEP_104 and WEP_40, use 24.</p>
end-date	Date and time user access expires.	<p>Date and time, in the following format: <i>YYMM/DD-HH:MM</i></p> <p>You can use end-date alone or with start-date. You also can use start-date, end-date, or both in conjunction with time-of-day.</p>

Table 44 Authentication Attributes for Local Users (continued)

filter-id	Inbound or outbound ACL to apply to the user.	<p>If configured in the WX local database, this attribute can be an access control list (ACL) to filter outbound or inbound traffic. Use the following format:</p> <p>filter-id <i>inboundacl.in</i></p> <p>or</p> <p>filter-id <i>outboundacl.out</i></p> <p>If you are configuring the attribute on a RADIUS server, the value field of filter-id can specify up to two ACLs. Any of the following are valid:</p> <pre>filter-id = "Profile=acl1 "</pre> <pre>filter-id = "OutboundACL=acl2 "</pre> <pre>filter-id = "Profile=acl1 OutboundACL=acl2 "</pre> <p>(Each example goes on a single line on the server.) The format in which to specify the values depends on the RADIUS server.</p> <p>Regardless of whether the attributes are defined locally or on a RADIUS server, the ACLs must already be configured on the WX.</p>
idle-timeout	This option is not implemented in the current MSS version.	
mobility-profile (network access mode only)	Mobility Profile attribute for the user. (For more information, see set mobility-profile on page 269.)	<p>Name of an existing Mobility Profile, up to 32 alphanumeric characters, with no tabs or spaces.</p> <p>Note: If the Mobility Profile feature is enabled, and a user is assigned a Mobility Profile name that does not exist on the WX, the user is denied access.</p>

Table 44 Authentication Attributes for Local Users (continued)

service-type	Type of access requested by the user.	<p>One of the following numbers:</p> <p>2—Framed; for network user access</p> <p>6—Administrative; for administrative access to the WX, with authorization to access the enabled (configuration) mode. The user must enter the enable command to access the enabled mode.</p> <p>7—NAS-Prompt; for administrative access to the nonenabled mode only. In this mode, the enable command is not available and the user cannot log in to the enabled mode.</p> <p>For administrative sessions, the WX always sends 6 (Administrative).</p> <p>The RADIUS server can reply with one of the values listed above.</p> <p>If the service-type is not set on the RADIUS server, administrative users receive NAS-Prompt access, and network users receive Framed access.</p>
session-timeout (network access mode only)	Maximum number of seconds for the user's session.	Number between 0 and 4,294,967,296 seconds (approximately 136.2 years).
ssid (network access mode only)	SSID accessible by the user after authentication.	Name of the SSID you want the user to use. The SSID must be configured in a service profile, and the service profile must be used by a radio profile assigned to MAP radios in the Mobility Domain.
start-date	<p>Date and time at which the user becomes eligible to access the network.</p> <p>MSS does not authenticate the user unless the attempt to access the network occurs at or after the specified date and time, but before the end-date (if specified).</p>	<p>Date and time, in the following format: YY/MM/DD-HH:MM</p> <p>You can use start-date alone or with end-date. You also can use start-date, end-date, or both in conjunction with time-of-day.</p>

Table 44 Authentication Attributes for Local Users (continued)

time-of-day (network access mode only)	Day(s) and time(s) during which the user is permitted to log into the network. After authorization, the user session can last until either the Time-Of-Day range or the Session-Timeout duration (if set) expires, whichever is shorter.	<p>One of the following:</p> <ul style="list-style-type: none"> ▪ never—Access is always denied. ▪ any—Access is always allowed. ▪ al—Access is always allowed. ▪ One or more ranges of values that consist of one of the following day designations (required), and a time range in <i>hhmm-hhmm</i> 4-digit 24-hour format (optional): <ul style="list-style-type: none"> mo—Monday tu—Tuesday we—Wednesday th—Thursday fr—Friday sa—Saturday su—Sunday wk—Any day between Monday and Friday <p>Separate values or a series of ranges (except time ranges) with commas (,) or a vertical bar (). Do not use spaces.</p> <p>The maximum number of characters is 253.</p> <p>For example, to allow access only on Tuesdays and Thursdays between 10 a.m. and 4 p.m., specify the following: time-of-day tu1000-1600,th1000-1600</p> <p>To allow access only on weekdays between 9 a.m and 5 p.m., and on Saturdays from 10 p.m. until 2 a.m., specify the following: time-of-day wk0900-1700,sa2200-0200</p> <p>(Also see the examples for set user attr on page 273.)</p> <p>You can use time-of-day in conjunction with start-date, end-date, or both.</p>
---	---	---

Table 44 Authentication Attributes for Local Users (continued)

url (network access mode only)	URL to redirect the user after successful WebAAA.	Web URL, in standard format. For example: http://www.example.com You must include the <i>http://</i> portion. You can dynamically include any of the variables in the URL string: <ul style="list-style-type: none"> ▪ \$u—Username ▪ \$v—VLAN ▪ \$s—SSID ▪ \$p—Service profile name To use the literal character \$ or ?, use the following: <ul style="list-style-type: none"> ▪ \$\$ ▪ \$q
vlan-name (network access mode only)	Virtual LAN (VLAN) assignment. On some RADIUS servers, you might need to use the standard RADIUS attribute Tunnel-Pvt-Group-ID, instead of VLAN-Name.	Name of a VLAN that you want the user to use. The VLAN must be configured on a WX within the Mobility Domain to which this WX belongs.
acct-interim-interval	Interval in seconds between accounting updates, if start-stop accounting mode is enabled.	Number between 180 and 3,600 seconds, or 0 to disable periodic accounting updates. The WX ignores the acct-interim-interval value and issues a log message if the value is below 60 seconds. If both a RADIUS server and the WX supply a value for the acct-interim-interval attribute, then the value from the WX takes precedence.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To change the value of an attribute, enter **set mac-user attr** with the new value. To delete an attribute, use **clear mac-user attr**.

You can assign attributes to individual MAC users and to MAC user groups. If attributes are configured for a MAC user and also for the group the MAC user is in, the attributes assigned to the individual MAC user take precedence for that user. For example, if the start-date attribute configured for a MAC user is sooner than the start-date configured for the MAC user group the user is in, the MAC user's network access can begin as soon as the user start-date. The MAC user does not need to wait for the MAC user group's start date.

Examples — The following command assigns input access control list (ACL) *acl-03* to filter packets from a user at MAC address 01:02:03:04:05:06:

```
WX4400# set mac-user 01:02:03:04:05:06 attr filter-id
acl-03.in
success: change accepted.
```

The following command restricts a user at MAC address 06:05:04:03:02:01 to network access between 7 p.m. on Mondays and Wednesdays and 7 a.m. on Tuesdays and Thursdays:

```
WX4400# set mac-user 06:05:04:03:02:01 attr time-of-day
mo1900-1159,tu0000-0700,we1900-1159,th0000-0700
success: change accepted.
```

See Also

- **clear mac-user attr** on page 221
- **display aaa** on page 229

set mac-usergroup attr

Creates a user group in the local database on the WX for users authenticated by a MAC address, and assigns authorization attributes for the group.

(To configure a user group and assign authorization attributes through RADIUS, see the documentation for your RADIUS server.)

Syntax — set mac-usergroup

group-name **attr** *attribute-name value*

- **group-name** — Name of a MAC user group. Specify a name of up to 32 alphanumeric characters, with no spaces.

- *attribute-name value* — Name and value of an attribute used to authorize all MAC users in the group for a particular service or session characteristic. (For a list of authorization attributes, see Table 44 on page 262.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To change the value of an attribute, enter **set mac-usergroup attr** with the new value. To delete an attribute, use **clear mac-usergroup attr**.

You can assign attributes to individual MAC users and to MAC user groups. If attributes are configured for a MAC user and also for the group of the MAC user, the attributes assigned to the individual MAC user take precedence for that user. For example, if the start-date attribute configured for a MAC user is earlier than the start-date configured for the MAC user group, the MAC user network access can begin as soon as the user start-date. The MAC user does not need to wait for the MAC user group start date.

Examples — The following command creates the MAC user group *eastcoasters* and assigns the group members to VLAN *orange*:

```
WX4400# set mac-usergroup eastcoasters attr vlan-name orange
success: change accepted.
```

See Also

- **clear mac-usergroup attr** on page 223
- **display aaa** on page 229

set mobility-profile Creates a Mobility Profile and specifies the MAP access point and/or wired authentication ports on the WX switch through which any user assigned to the profile is allowed access.

Syntax — `set mobility-profile name name {port {none | all | port-list}} | {ap {none | all | ap-num}}`

- *name* — Name of the Mobility Profile. Specify up to 32 alphanumeric characters, with no spaces.
- **none** — Prevents any user to whom this profile is assigned from accessing any MAP access point or wired authentication port on the WX switch.
- **all** — Allows any user to whom this profile is assigned to access all MAP access ports and wired authentication port on the WX switch.
- *port-list* — List of MAP access ports or wired authentication ports through which any user assigned this profile is allowed access. The same port can be used in multiple Mobility Profile port lists.
- *ap-num* — List of Distributed MAP connections through which any user assigned this profile is allowed access. The same Distributed MAP can be used in multiple Mobility Profile port lists.

Defaults — No default Mobility Profile exists on the WX. If you do not assign Mobility Profile attributes, all users have access through all ports, unless denied access by other AAA servers or by access control lists (ACLs).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To assign a Mobility Profile to a user or group, specify it as an authorization attribute in one of the following commands:

```
set user attr mobility-profile name
set usergroup attr mobility-profile name
set mac-user attr mobility-profile name
set mac-usergroup attr mobility-profile name
```

To enable the use of the Mobility Profile feature on the WX switch, use the **set mobility-profile mode** command.



CAUTION: When the Mobility Profile feature is enabled, a user is denied access if assigned a Mobility-Profile attribute in the local WX database or RADIUS server when no Mobility Profile of that name exists on the WX.

To change the ports in a profile, use **set mobility-profile** again with the updated port list.

Examples — The following commands create the Mobility Profile *magnolia*, which restricts user access to port 2; enable the Mobility Profile feature on the WX switch; and assign the *magnolia* Mobility Profile to user *Jose*.

```
WX1200# set mobility-profile name magnolia port 2
success: change accepted.
WX1200# set mobility-profile mode enable
success: change accepted.
WX1200# set user Jose attr mobility-profile magnolia
success: change accepted.
```

The following command adds port 3 to the *magnolia* Mobility Profile (which is already assigned to port 2):

```
WX1200# set mobility-profile name magnolia port 3
success: change accepted.
```

See Also

- **clear mobility-profile** on page 224
- **display mobility-profile** on page 235
- **set mac-user attr** on page 261
- **set mac-usergroup attr** on page 267
- **set mobility-profile mode** on page 271
- **set user attr** on page 273
- **set usergroup** on page 275

set mobility-profile mode

Enables or disables the Mobility Profile feature on the WX switch.



CAUTION: When the Mobility Profile feature is enabled, a user is denied access if assigned a Mobility-Profile attribute in the local WX database or RADIUS server when no Mobility Profile of that name exists on the WX.

Syntax — `set mobility-profile mode {enable | disable}`

- **enable** — Enables the use of the Mobility Profile feature on the WX.
- **disable** — Specifies that all Mobility Profile attributes are ignored by the WX.

Defaults — The Mobility Profile feature is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To enable the use of the Mobility Profile feature, type the following command:

```
WX1200# set mobility-profile mode enable
success: change accepted.
```

See Also

- **clear mobility-profile** on page 224
- **display mobility-profile** on page 235
- **set mobility-profile** on page 269

set user

Configures a user profile in the local database on the WX for a user with a password.

(To configure a user profile in RADIUS, see the documentation for your RADIUS server.)

Syntax — `set user username password [encrypted] string`

- *username* — Username of a user with a password.

- **encrypted** — Indicates that the password string you entered is already in its encrypted form. If you use this option, MSS does not encrypt the displayed form of the password string, and instead displays the string exactly as you entered it. If you omit this option, MSS does encrypt the displayed form of the string.
- **password *string*** — Password of up to 32 alphanumeric characters, with no spaces.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Although MSS allows you to configure a user password for the special “last-resort” guest user, the password has no effect. Last-resort users can never access a WX in administrative mode and never require a password.

Examples — The following command creates a user profile for user Nin in the local database, and assigns the password *goody*:

```
WX4400# set user Nin password goody
success: User Nin created
```

The following command assigns the password *chey3nne* to the **admin** user:

```
WX4400# set user admin password chey3nne
success: User admin created
```

The following command changes Nin’s password from *goody* to *29Jan04*:

```
WX4400# set user Nin password 29Jan04
```

See Also

- **clear user** on page 224
- **display aaa** on page 229

set user attr

Configures an authorization attribute in the local database on the WX switch for a user with a password.

(To assign authorization attributes in RADIUS, see the documentation for your RADIUS server.)

Syntax — `set user username attr attribute-name value`

- *username* — Username of a user with a password.
- *attribute-name value* — Name and value of an attribute you are using to authorize the user for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to network users, see Table 44 on page 262.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To change the value of an attribute, enter **set user attr** with the new value. To delete an attribute, use **clear user attr**.

You can assign attributes to individual users and to user groups. If attributes are configured for a user and also for the group the user is in, the attributes assigned to the individual user take precedence for that user. For example, if the start-date attribute configured for a user is sooner than the start-date configured for the user group the user is in, the user's network access can begin as soon as the user start-date. The user does not need to wait for the user group's start date.

Examples — The following command assigns user Tamara to VLAN *orange*:

```
WX4400# set user Tamara attr vlan-name orange
success: change accepted.
```

The following command assigns Tamara to the Mobility Profile *tulip*.

```
WX4400# set user Tamara attr mobility-profile tulip
success: change accepted.
```

The following command limits the days and times when user Student1 can access the network, to 5 p.m. to 2 a.m. every weekday, and all day Saturday and Sunday:

```
WX4400# set user Student1 attr time-of-day Wk1700-0200,Sa,Su
success: change accepted.
```

See Also

- **clear user attr** on page 225
- **display aaa** on page 229

set user expire-password-in

Specifies how long a user password is valid before it must be reset.

Syntax `set user username expire-password-in time`

- *username* — Username of a user with a password.
- *time* — How long the specified user's password is valid. The amount of time can be specified in days (for example, *30* or *30d*), hours (720h), or a combination of days and hours (30d12h).

Defaults — By default, user passwords do not expire.

Access — Enabled.

History — Introduced in MSS 6.0.

Usage — Use this command to specify how long a specified user's password is valid. After this amount of time, the user's password expires, and a new password must be set.

Examples — The following command sets user Student1's password to be valid for 30 days:

```
WX# set user Student1 expire-password-in 30
success: change accepted.
```

See Also

- **clear user lockout** on page 226
- **set authentication minimum-password-length** on page 251
- **set authentication password-restrict** on page 252
- **set user** on page 271

set user group

Adds a user to a user group. The user must have a password and a profile that exists in the local database on the WX.

(To configure a user in RADIUS, see the documentation for your RADIUS server.)

Syntax — `set user username group group-name`

- *username* — Username of a user with a password.
- *group-name* — Name of an existing user group for password users.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — MSS does not require users to belong to user groups.

To *create* a user group, use the command **set usergroup**.

Examples — The following command adds user Hosni to the *cardiology* user group:

```
WX4400# set user Hosni group cardiology
success: change accepted.
```

See Also

- **clear user group** on page 226
- **display aaa** on page 229

set usergroup

Creates a user group in the local database on the WX for users and assigns authorization attributes for the group.

(To create user groups and assign authorization attributes in RADIUS, see the documentation for your RADIUS server.)

Syntax — `set usergroup group-name attr attribute-name value`

- *group-name* — Name of a group for password users. Specify a name of up to 32 alphanumeric characters, with no spaces.

- *attribute-name value* — Name and value of an attribute you are using to authorize all users in the group for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to users, see Table 44 on page 262.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To change the value of an attribute, enter **set usergroup attr** with the new value. To delete an attribute, use **clear usergroup attr**.

To *add* a user to a group, use the command **set user group**.

You can assign attributes to individual users and to user groups. If attributes are configured for a user and also for the group the user is in, the attributes assigned to the individual user take precedence for that user. For example, if the start-date attribute configured for a user is sooner than the start-date configured for the user group the user is in, the user's network access can begin as soon as the user start-date. The user does not need to wait for the user group's start date.

Examples — The following command adds the user group *cardiology* to the local database and assigns all the group members to VLAN *crimson*:

```
WX4400# set usergroup cardiology attr vlan-name crimson
success: change accepted.
```

See Also

- **clear usergroup** on page 227
- **clear usergroup attr** on page 228
- **display aaa** on page 229

**set usergroup
expire-password-in**

Specifies how long the passwords for the users in user group are valid before they must be reset.

Syntax `set usergroup group-name expire-password-in time`

- *group-name* — Name of a group for password users.
- *time* — How long the passwords for the users in the specified group are valid. The amount of time can be specified in days (for example, *30* or *30d*), hours (*720h*), or a combination of days and hours (*30d12h*).

Defaults — By default, user passwords do not expire.

Access — Enabled.

History — Introduced in MSS 6.0.

Usage — Use this command to specify how long the passwords for the users in a group are valid. After this amount of time, the passwords expire, and must be reset.

Examples — The following command sets the passwords for the users in user group *cardiology* to be valid for 30 days:

```
WX# set usergroup cardiology expire-password-in 30
success: change accepted.
```

See Also

- **clear user lockout** on page 226
- **set authentication minimum-password-length** on page 251
- **set authentication password-restrict** on page 252
- **set user** on page 271

set web-portal

Globally enables or disables WebAAA on a WX switch.

Syntax — `set web-portal {enable | disable}`

- **enable** — Enables WebAAA on the switch.
- **disable** — Disables WebAAA on the switch.

Defaults — Enabled.

Access — Enabled.

History — Introduced in MSS Version 3.0. Command name changed from **set web-aaa** to **set web-portal**, to match change to portal-based implementation in MSS Version 4.0.

Usage — This command disables or reenables support for WebAAA. However, WebAAA has additional configuration requirements. For information, see the “Configuring AAA for Network Users” chapter in the *Wireless LAN Switch and Controller Configuration Guide*.

Examples — To disable WebAAA, type the following command:

```
WX4400# set web-portal disable
success: change accepted.
```

See Also

- **clear authentication proxy** on page 218
- **set service-profile auth-fallthru** on page 434
- **set user** on page 271

9

MOBILITY DOMAIN COMMANDS

Use Mobility Domain commands to configure and manage Mobility Domain groups.

A Mobility Domain is a system of WX switches and MAP access points working together to support a roaming user (client). One WX acts as a seed switch, which maintains and distributes a list of IP addresses of the domain members.



3Com recommends that you run the same MSS version on all the WX switches in a Mobility Domain.

Commands by Usage

This chapter presents Mobility Domain commands alphabetically. Use Table 45 to locate commands in this chapter based on their use.

Table 45 Mobility Domain Commands by Usage

Type	Command
Mobility Domain	set mobility-domain mode seed domain-name on page 288
	set mobility-domain member on page 284
	set mobility-domain mode member seed-ip on page 286
	set mobility-domain mode secondary-seed domain-name on page 287
	display mobility-domain on page 281
	display mobility-domain status on page 283
	display mobility-domain config on page 282
	display mobility-domain status on page 283
	clear mobility-domain member on page 280
	clear mobility-domain on page 280
	set domain security on page 289

**clear
mobility-domain**

Clears all Mobility Domain configuration and information from a WX , regardless of whether the WX is a seed or a member of a Mobility Domain.

Syntax — `clear mobility-domain`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command has no effect if the WX is not configured as part of a Mobility Domain.

Examples — To clear a Mobility Domain from a WX within the domain, type the following command:

```
WX1200# clear mobility-domain
success: change accepted.
```

See Also

- **clear mobility-domain member** on page 280
- **set mobility-domain member** on page 284
- **set mobility-domain mode member seed-ip** on page 286
- **set mobility-domain mode seed domain-name** on page 288

**clear
mobility-domain
member**

On the seed WX, removes the identified member from the Mobility Domain.

Syntax — `clear mobility-domain member ip-addr`

- *ip-addr* — IP address of the Mobility Domain member, in dotted decimal notation.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command has no effect if the WX member is not configured as part of a Mobility Domain or the current WX is not the seed.

Examples — The following command clears a Mobility Domain member with the IP address 192.168.0.1:

```
WX1200# clear mobility-domain member 192.168.0.1
```

See Also

- **set mobility-domain member** on page 284

display mobility-domain

On the seed WX, displays the Mobility Domain status and members.

Syntax — `display mobility-domain`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 1.0.

Examples — To display Mobility Domain status, type the following command:

```
WX# display mobility-domain
Mobility Domain name: Pleasanton (security required)
Member      State      Type(*:active)  Model      Version
-----
10.8.107.1  STATE_UP   SEED*           WX-20      6.0.1.0
10.10.10.66 STATE_DOWN  MEMBER          Unknown    Unknown
```

Table 46 display mobility-domain Output

Field	Description
Mobility Domain name	Name of the Mobility Domain
Member	IP addresses of the seed WX and members in the Mobility Domain
State	State of the WX in the Mobility Domain: <ul style="list-style-type: none"> ▪ STATE_UP ▪ STATE_DOWN

Table 46 display mobility-domain Output

Field	Description
Type	Role of the WX in the Mobility Domain: <ul style="list-style-type: none"> ▪ MEMBER ▪ SEED ▪ SECONDARY-SEED
Model	Mode of the WX
Version	MSS version running on the WX

See Also

- **clear mobility-domain** on page 280
- **set mobility-domain member** on page 284
- **set mobility-domain mode member seed-ip** on page 286

**display
mobility-domain
config**

Displays the configuration of the Mobility Domain.

Syntax — `display mobility-domain config`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command displays the Mobility Domain configuration:

```
WX# display mobility-domain config
This switch is the seed for domain dang-modo.
10.8.107.1 is a member
10.10.10.66 is a member
```

See Also

- **clear mobility-domain** on page 280
- **display mobility-domain status** on page 283
- **set mobility-domain member** on page 284

display mobility-domain status

On the seed WX, displays the Mobility Domain status and members.

Syntax — `display mobility-domain status`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To display Mobility Domain status, type the following command:

```
WX4400# display mobility-domain status
Mobility Domain name: Pleasanton
Member                State                Status
-----
192.168.253.11       STATE_UP            MEMBER
192.168.253.12       STATE_DOWN          MEMBER
192.168.253.14       STATE_UP            SEED
```

Table 47 describes the fields in the display.

Table 47 display mobility-domain Output

Field	Description
Mobility Domain name	Name of the Mobility Domain
Member	IP addresses of the seed WX switch and members in the Mobility Domain
State	State of the WX switch in the Mobility Domain: <ul style="list-style-type: none"> ▪ STATE_UP ▪ STATE_DOWN
Status	Role of the WX switch in the Mobility Domain: <ul style="list-style-type: none"> ▪ MEMBER ▪ SEED

See Also

- **clear mobility-domain** on page 280
- **set mobility-domain member** on page 284
- **set mobility-domain mode member seed-ip** on page 286

**set
mobility-domain
member**

On the seed WX, adds a member to the list of Mobility Domain members. If the current WX is not configured as a seed, this command is rejected.

Syntax — `set mobility-domain member ip-addr Key hex-bytes`

- *ip-addr* — IP address of the Mobility Domain member in dotted decimal notation.
- *key hex-bytes* — Fingerprint of the public key to use for WX-WX security. Specify the key as 16 hexadecimal bytes. Use a colon between each byte, as in the following example:
00:11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee:ff.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command must be entered from the seed WX.

Examples — The following commands add three WX switches with the IP addresses 192.168.1.8, 192.168.1.9, and 192.168.1.10 as members of a Mobility Domain whose seed is the current WX:

```
WX4400# set mobility-domain member 192.168.1.8
success: change accepted.
WX4400# set mobility-domain member 192.168.1.9
success: change accepted.
WX4400# set mobility-domain member 192.168.1.10
success: change accepted.
```

See Also

- **clear mobility-domain member** on page 280
- **display mobility-domain config** on page 282
- **set mobility-domain mode seed domain-name** on page 288

**set
mobility-domain
mode member
secondary seed-ip**

Sets the IP address of the secondary seed WX on a nonseed WX.

Syntax — `set mobility-domain mode member secondary seed-ip secondary-seed-ip-addr key hex-bytes`

- `secondary-seed-ip-addr` — IP address of the secondary seed, in dotted decimal notation.
- `key hex-bytes` — Fingerprint of the public key to use for WX-WX security. Specify the key as 16 hexadecimal bytes. Use a colon between each byte, as in the following example:
00:11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee:ff.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 1.0.

Examples — The following command sets the current WX switch as a nonseed member of the Mobility Domain whose secondary seed has the IP address 192.168.1.8:

```
WX4400# set mobility-domain mode member seed-ip 192.168.1.8
mode is: member
seed IP is: 192.168.1.8
```

See Also

- **clear mobility-domain** on page 280
- **display mobility-domain config** on page 282

**set
mobility-domain
mode member
seed-ip**

On a nonseed WX, sets the IP address of the seed WX. This command is used on a member WX to configure it as a member. If the WX is currently part of another Mobility Domain or using another seed, this command overwrites that configuration.

Syntax — `set mobility-domain mode member seed-ip ip-addr key hex-bytes`

- *ip-addr* — IP address of the Mobility Domain member, in dotted decimal notation.
- *key* *hex-bytes* — Fingerprint of the public key to use for WX-WX security. Specify the key as 16 hexadecimal bytes. Use a colon between each byte, as in the following example:
00:11:22:33:44:55:66:77:88:99:aa:bb:cc:dd:ee:ff.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 1.0. Option key hex-bytes added in Version 5.0.

Examples — The following command sets the current WX as a nonseed member of the Mobility Domain whose seed has the IP address 192.168.1.8:

```
WX# set mobility-domain mode member secondary seed-ip  
192.168.1.8
```

See Also

- **clear mobility-domain** on page 280
- **display mobility-domain config** on page 282

**set
mobility-domain
mode
secondary-seed
domain-name**

Sets the current WX as a secondary-seed device for the Mobility Domain.

Syntax — `set mobility-domain mode secondary-seed domain-name
mob-domain-name seed-ip primary-seed-ip-addr`

- *mob-domain-name* — Name of the Mobility Domain. Specify between 1 and 32 characters with no spaces.
- *primary-seed-ip-addr* — The address of the seed device in the Mobility Domain

Defaults — None.

Access — Enabled.

History — Introduced in MSS 6.0.

Usage — You can optionally specify a secondary seed in a Mobility Domain. The secondary seed provides redundancy for the primary seed switch in the Mobility Domain. If the primary seed becomes unavailable, the secondary seed assumes the role of the seed switch. This allows the Mobility Domain to continue functioning if the primary seed becomes unavailable.

When the primary seed switch fails, the remaining members form a Mobility Domain, with the secondary seed taking over as the primary seed switch.

If countermeasures had been in effect on the primary seed, they are stopped while the secondary seed gathers RF data from the member switches. Once the secondary seed has rebuilt the RF database, countermeasures can be restored.

VLAN tunnels (other than those between the member switches and the primary seed) continue to operate normally.

Roaming and session statistics continue to be gathered, providing that the primary seed is uninvolved with roaming.

When the primary seed is restored, it resumes its role as the primary seed switch in the Mobility Domain. The secondary seed returns to its role as a regular member of the Mobility Domain.

Examples — The following command configures this WX as the secondary seed in a Mobility Domain named Pleasanton:

```
WX# set mobility-domain mode secondary-seed domain-name
Pleasanton
mode is: secondary-seed
domain name is: Pleasanton
```

See Also

- **clear mobility-domain member** on page 280
- **display mobility-domain** on page 281

set mobility-domain mode seed domain-name

Creates a Mobility Domain by setting the current WX as the seed device and naming the Mobility Domain.

Syntax — `set mobility-domain mode seed domain-name`
mob-domain-name

- *mob-domain-name* — Name of the Mobility Domain. Specify between 1 and 32 characters with no spaces.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. Version 4.2 increased the maximum length of *mob-domain-name* to 32 characters.

Usage — Before you use this command, the current WX must have its IP address set with the **set system ip-address** command. After you enter this command, all Mobility Domain traffic is sent and received from the specified IP address.

You must explicitly configure *only one* WX switch per domain as the seed. All other WX switches in the domain receive their Mobility Domain information from the seed.

Examples — The following command creates a Mobility Domain named Pleasanton with the current WX as the seed:

```
WX4400# set mobility-domain mode seed domain-name Pleasanton
mode is: seed
domain name is: Pleasanton
```


See Also

- **clear mobility-domain member** on page 280
- **display mobility-domain status** on page 283

set domain security

Sets mobility domain security to required (enabled) or none (disabled) on the wireless LAN switch. The command needs to be entered on each wireless LAN switch that will participate as a member of the secure mobility domain.

Syntax — `set domain security {required | none}`

Defaults — Mobility domain security is disabled by default.

Access — Enabled.

History — Introduced in MSS 5.0.

Usage — Domain keys for all switches must be properly configured before enabling domain security on the wireless LAN switch.

Examples — The following command enables mobility domain security on the wireless LAN switch:

```
WX4400# set domain security required
success: change accepted.
```


10

NETWORK DOMAIN COMMANDS

Use Network Domain commands to configure and manage Network Domain groups.

A Network Domain is a group of geographically dispersed Mobility Domains that share information over a WAN link. This shared information allows a user configured on a WX in one Mobility Domain to establish connectivity on a WX in another Mobility Domain in the same Network Domain. The WX forwards the user traffic by creating a VLAN tunnel to a WX in the remote Mobility Domain.

In a Network Domain, one or more WX switches serve as a seed switch. At least one of the Network Domain seeds maintains a connection with each of the member WX switches in the Network Domain. The Network Domain seeds share information about the VLANs configured on their members, so that all the Network Domain seeds have a common database of VLAN information.

Network Domain Commands by Usage

This chapter presents Network Domain commands alphabetically. Use Table 48 to locate commands in this chapter based on their use.

Table 48 Network Domain Commands by Usage

Type	Command
Network Domain	set network-domain mode seed domain-name on page 300
	set network-domain mode member seed-ip on page 298
	set network-domain peer on page 299
	clear network-domain on page 292
	clear network-domain mode on page 293

Table 48 Network Domain Commands by Usage (continued)

Type	Command
	clear network-domain peer on page 294
	clear network-domain seed-ip on page 295
	display network-domain on page 296

clear network-domain

Clears all Network Domain configuration and information from a WX , regardless of whether the WX is a seed or a member of a Network Domain.

Syntax — `clear network-domain`

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.1.

Examples — This command has no effect if the WX is not configured as part of a Network Domain.

To clear a Network Domain from a WX within the domain, type the following command:

```
WX1200# clear network-domain
This will clear all network-domain configuration. Would you
like to continue? (y/n) [n] y
success: change accepted.
```

See Also

- **set network-domain mode member seed-ip** on page 298
- **set network-domain peer** on page 299
- **set network-domain mode seed domain-name** on page 300

**clear
network-domain
mode**

Removes the Network Domain seed or member configuration from the WX.

Syntax — `clear network-domain mode {seed | member}`

- **seed** — Clears the Network Domain seed configuration from the WX switch.
- **member** — Clears the Network Domain member configuration from the WXswitch.

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.1.

Usage — This command has no effect if the WX is not configured as part of a Network Domain.

Examples — The following command clears the Network Domain member configuration from the WX:

```
WX1200# clear network-domain mode member
success: change accepted.
```

The following command clears the Network Domain seed configuration from the WX:

```
WX1200# clear network-domain mode seed
success: change accepted.
```

See Also

- **set network-domain mode member seed-ip** on page 298
- **set network-domain mode seed domain-name** on page 300

**clear
network-domain
peer**

Removes the configuration of a Network Domain peer from a WX configured as a Network Domain seed.

Syntax — `clear network-domain peer {ip-addr | all}`

- *ip-addr* — IP address of the Network Domain peer in dotted decimal notation.
- **all** — Clears the Network Domain peer configuration for all peers from the WX switch.

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.1.

Usage — This command has no effect if the WX is not configured as a Network Domain seed.

Examples — The following command clears the Network Domain peer configuration for peer 192.168.9.254 from the WX:

```
WX1200# clear network-domain peer 192.168.9.254
success: change accepted.
```

The following command clears the Network Domain peer configuration for all peers from the WX:

```
WX1200# clear network-domain peer all
success: change accepted.
```

See Also

- **set network-domain peer** on page 299

**clear
network-domain
seed-ip**

Removes the specified Network Domain seed from the WX configuration. When you enter this command, the Network Domain TCP connections between the WX switch and the specified Network Domain seed are closed.

Syntax — `clear network-domain seed-ip ip-addr`

- *ip-addr* — IP address of the Network Domain seed in dotted decimal notation.

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.1.

Usage — This command has no effect if the WX is not configured as part of a Network Domain, or if the WX is not configured as a member of a Network Domain that uses the specified Network Domain seed.

The following command removes the Network Domain seed with IP address 192.168.9.254 from the WX configuration:

```
WX1200# clear network-domain seed-ip 192.168.9.254
success: change accepted.
```

See Also

- **set network-domain mode member seed-ip** on page 298

**display
network-domain**

Displays the status of Network Domain seeds and members.

Syntax — `display network-domain`

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.1.

Examples — To display Network Domain status, type the following command. The output of the command differs based on whether the WX switch is a member of a Network Domain or a Network Domain seed.

On a WX that is a Network Domain member, the following output is displayed:

```
WX1200# display network-domain
Member Network Domain name: California
Member      State      Mode
-----
10.8.107.1   UP        SEED
```

On a WX switch that is a Network Domain seed, information is displayed about the Network Domains of which the WX switch is a member, as well as Network Domain seeds with which the WX switch has a peer relationship. For example:

```
WX1200# display network-domain
Network Domain name: California
Peer          State
-----
10.8.107.1    UP
Member      State      Mode
-----
10.1.0.0      DOWN      SEED
Member Network Domain name:
Member      State      Mode
-----
10.8.107.1   UP        MEMBER
10.1.0.0     DOWN      SEED
```


Table 49 describes the fields in the display.

Table 49 Radio-Specific Parameters

Parameter	Description
Output if WX is the Network Domain Seed	
Network Domain name	Name of the Network Domain for which the WX is a seed.
Peer	IP addresses of the other seeds in the Network Domain.
State	State of the connection between the WX and the peer Network Domain seeds: <ul style="list-style-type: none"> ▪ UP ▪ DOWN
Member	IP addresses of the seed WX and members in the Network Domain.
State	State of the WX in the Network Domain: <ul style="list-style-type: none"> ▪ UP ▪ DOWN
Mode	Role of the WX in the Network Domain: <ul style="list-style-type: none"> ▪ UP ▪ DOWN
Mobility-Domain	Name of the Mobility Domain of which the WX is a member.
Output if WX is a Network Domain Member	
Member Network Domain name	Name of the Network Domain of which the WX is a member.
Member	IP addresses of the seed WX and members in the Network Domain.
State	State of the WX in the Network Domain. <ul style="list-style-type: none"> ▪ UP ▪ DOWN
Mode	Role of the WX in the Network Domain: <ul style="list-style-type: none"> ▪ MEMBER ▪ SEED
Mobility-Domain	Name of the Mobility Domain of which the WX is a member.

See Also

- **clear network-domain** on page 292
- **set network-domain mode member seed-ip** on page 298
- **set network-domain mode seed domain-name** on page 300
- **set network-domain peer** on page 299

**set
network-domain
mode member
seed-ip**

Sets the IP address of a Network Domain seed. This command is used for configuring a WX as a member of a Network Domain. You can specify multiple Network Domain seeds and configure one as the primary seed.

Syntax — `set network-domain mode member seed-ip ip-addr [affinity num]`

- *ip-addr* — IP address of the Network Domain seed, in dotted decimal notation.
- *num* — Preference for using the specified Network Domain seed. You can specify a value from 1 through 10. A higher number indicates a greater preference.

Defaults — The default affinity for a Network Domain seed is 5.

Access — Enabled.

History — Introduced in MSS 4.1.

Usage — You can specify multiple Network Domain seeds on the WX. When the WX needs to connect to a Network Domain seed, it first attempts to connect to the seed with the highest affinity. If that seed is unavailable, the WX attempts to connect to the seed with the next-highest affinity. After a connection is made to a non-highest-affinity seed, the WX switch then periodically attempts to connect to the highest-affinity seed.

Examples — The following command sets the WX switch as a member of the Network Domain whose seed has the IP address 192.168.1.8:

```
WX1200# set network-domain mode member seed-ip 192.168.1.8
success: change accepted.
```

The following command sets the WX as a member of a Network Domain whose seed has the IP address 192.168.9.254 and sets the affinity for that seed to 7. If the WX specifies other Network Domain seeds, and they are configured with the default affinity of 5, then 192.168.9.254 becomes the primary Network Domain seed for this WX.

```
WX1200# set network-domain mode member seed-ip 192.168.9.254
affinity 7
success: change accepted.
```

See Also

- **clear network-domain** on page 292
- **display network-domain** on page 296

set network-domain peer

On a Network Domain seed, configures one or more WX as redundant Network Domain seeds. The seeds in a Network Domain share information about the VLANs configured on the member devices, so that all the Network Domain seeds have the same database of VLAN information.

Syntax — `set network-domain peer ip-addr`

- *ip-addr* — IP address of the Network Domain seed to specify as a peer, in dotted decimal notation.

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.1.

Usage — This command must be entered on a WX configured as a Network Domain seed.

Examples — The following command sets the WX switch with IP address 192.168.9.254 as a peer of this Network Domain seed:

```
WX1200# set network-domain peer 192.168.9.254
success: change accepted.
```

See Also

- **clear network-domain** on page 292
- **display network-domain** on page 296

**set
network-domain
mode seed
domain-name**

Creates a Network Domain by setting the current WX as a seed device and naming the Network Domain.

Syntax — `set network-domain mode seed domain-name
net-domain-name`

- *net-domain-name* — Name of the Network Domain. Specify between 1 and 16 characters with no spaces.

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.1.

Usage — Before you use this command, the current WX must have its IP address set with the **set system ip-address** command. After you enter this command, Network Domain traffic is sent and received from the specified IP address.

You can configure multiple WX switches as Network Domain seeds. If you do this, you must identify them as peers by using the **set network domain peer** command.

Examples — The following command creates a Network Domain named California with the current WX as a seed:

```
WX1200# set network-domain mode seed domain-name California
success: change accepted.
```



The seed switch in a Network Domain must also be configured as a member of the Network Domain, with the specified seed IP address pointing to the seed itself.

```
set network-domain mode member seed-ip ip-addr [affinity num]
```

For example, the following command sets the current WX switch as a member of a Network Domain where the WX switch with IP address 192.168.9.254 is a seed:

```
WX1200# set network-domain mode member seed-ip 192.168.9.254
success: change accepted.
```

See Also

- **clear network-domain** on page 292
- **display network-domain** on page 296

11

MANAGED ACCESS POINT COMMANDS

Use MAP access point commands to configure and manage MAP access points. Be sure to do the following before using the commands:

- Define the country-specific IEEE 802.11 regulations on the WX switch. (See **set system countrycode** on page 61.)
- Install the MAP access point and connect it to a port on the WX switch.
- Configure a MAP as a directly connected MAP or a Distributed MAP. (See **set port type ap** on page 97 and **set ap** on page 87.)



CAUTION: *Changing the system country code after MAP configuration disables MAP access points and deletes their configuration. If you change the country code on a WX, you must reconfigure all MAP access points.*

MAP Access Point Commands by Usage

This chapter presents MAP access point commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Table 50 Map Access Point Commands by Usage

Type	Command
Automatic Configuration of Distributed MAPs	set ap auto on page 362
	set ap auto mode on page 366
	set ap auto radiotype on page 365
	set ap auto persistent on page 364
	set ap bias on page 367
	set ap blink on page 368
	set ap group on page 379
	set ap radio auto-tune max-power on page 384

Table 50 Map Access Point Commands by Usage (continued)

Type	Command
	set ap radio auto-tune max-retransmissions on page 385
	set ap radio link-calibration on page 388
	set ap radio mode on page 391
	set ap radio radio-profile on page 392
	set ap auto radiotype on page 365
	set ap upgrade-firmware on page 396
External Antennas	set ap radio antennatype on page 383
	set ap radio antenna-location on page 382
MAP-WX Security	set ap fingerprint on page 376
	set ap security on page 395
Static IP Address Assignment for Distributed MAPs	set ap boot-configuration ip on page 369
	set ap boot-configuration switch on page 374
	set ap boot-configuration vlan on page 375
	clear ap boot-configuration on page 310
	display ap boot-configuration on page 342
	set ap upgrade-firmware on page 396
Radio Profile Assignment	set ap radio radio-profile on page 392
	set radio-profile mode on page 416
	clear radio-profile on page 312
	set radio-profile service-profile on page 424
	display radio-profile on page 350
SSID Assignment	set service-profile ssid-name on page 465
	set service-profile ssid-type on page 466
	set service-profile beacon on page 436
Radio Properties	set radio-profile active-scan on page 400
	set radio-profile beacon-interval on page 409
	set radio-profile countermeasures on page 410
	set radio-profile dtim-interval on page 412
	set radio-profile frag-threshold on page 413
	set radio-profile max-rx-lifetime on page 414

Table 50 Map Access Point Commands by Usage (continued)

Type	Command
	set radio-profile max-tx-lifetime on page 415
	set radio-profile preamble-length on page 419
	set radio-profile rts-threshold on page 423
Authentication and Encryption	set service-profile attr on page 431
	set service-profile auth-dot1x on page 433
	set service-profile auth-fallthru on page 434
	set service-profile web-portal-form on page 473
	set service-profile web-portal-acl on page 472
	set service-profile auth-psk on page 435
	set service-profile wpa-ie on page 481
	set service-profile rsn-ie on page 455
	set service-profile cipher-ccmp on page 440
	set service-profile cipher-tkip on page 441
	set service-profile cipher-wep104 on page 442
	set service-profile cipher-wep40 on page 443
	set service-profile psk-phrase on page 453
	set service-profile psk-raw on page 454
	set service-profile tkip-mc-time on page 466
	set service-profile wep active-multicast- index on page 478
	set service-profile wep active-unicast- index on page 479
	set service-profile wep key-index on page 480
	set service-profile keep-initial-vlan on page 447
	set service-profile transmit-rates on page 468
	set service-profile long-retry-count on page 449
	set service-profile short-retry-count on page 456
	set service-profile shared-key-auth on page 456
	display service-profile on page 353
	clear service-profile on page 313

Table 50 Map Access Point Commands by Usage (continued)

Type	Command
QoS and VoIP	set radio-profile qos-mode on page 420
	set radio-profile wmm-powersave on page 430
	set service-profile cac-mode on page 438
	set service-profile cac-session on page 439
	set service-profile static-cos on page 467
	set service-profile cos on page 444
	set service-profile use-client-dscp on page 470
DHCP Restrict	set service-profile dhcp-restrict on page 445
Broadcast Control	set service-profile no-broadcast on page 451
Proxy ARP	set service-profile proxy-arp on page 452
Keepalives and Session Timers	set service-profile idle-client-probing on page 446
	set service-profile user-idle-timeout on page 471
	set service-profile web-portal-session-timeout on page 477
Sygate On-Demand (SODA)	set service-profile soda mode on page 462
	set service-profile soda agent-directory on page 457
	set service-profile soda enforce-checks on page 458
	set service-profile soda failure-page on page 459
	set service-profile soda remediation-ad on page 463
	set service-profile soda success-page on page 464
	set service-profile soda logout-page on page 460
Radio Transmit Rates	set service-profile transmit-rates on page 468
	set radio-profile rate-enforcement on page 421
Transmit Retries	set service-profile long-retry-count on page 449
	set service-profile short-retry-count on page 456
RF Auto-Tuning	set radio-profile auto-tune 11a-channel-range on page 401
	set radio-profile auto-tune channel-holddown on page 403
	set radio-profile auto-tune channel-interval on page 404

Table 50 Map Access Point Commands by Usage (continued)

Type	Command
	set radio-profile auto-tune channel-lockdown on page 405
	set radio-profile auto-tune power-config on page 406
	set radio-profile auto-tune power-interval on page 407
	set radio-profile auto-tune power-lockdown on page 408
	set ap radio auto-tune max-power on page 384
	display auto-tune neighbors on page 340
	display auto-tune attributes on page 338
AeroScout Tag Support	set radio-profile rfid-mode on page 421
Radio State	set ap radio mode on page 391
Dual Homing	set ap bias on page 367
RF Load Balancing	set ap radio load balancing on page 389
	clear ap radio load-balancing group on page 311
	set band-preference on page 397
	set load-balancing mode on page 398
	set load-balancing strictness on page 399
	set service-profile load-balancing- exempt on page 448
	display load-balancing group on page 348
MAP Administration and Maintenance	set ap name on page 381
	set ap blink on page 368
	set ap upgrade-firmware on page 396
	set ap force-image- download on page 378
	reset ap on page 362
	set ap radio channel on page 387
	set ap radio tx-power on page 393
	clear ap radio on page 308
	display ap config on page 316
	display ap status on page 331
	display ap counters on page 319
	display ap global on page 345
	display ap connection on page 343

Table 50 Map Access Point Commands by Usage (continued)

Type	Command
	display ap unconfigured on page 347
	display ap qos-stats on page 326
	display ap etherstats on page 327
MAP Local Switching	set ap local-switching mode on page 379
	set ap local-switching vlan-profile on page 380
	clear ap local-switching vlan-profile on page 307
	display ap arp on page 314
	display ap fdb on page 325
	display ap vlan on page 337
WLAN Mesh Services	set ap boot- configuration mesh mode on page 370
	set ap boot-configuration mesh psk-phrase on page 371
	set ap boot-configuration mesh psk-raw on page 372
	set ap boot-configuration mesh ssid on page 373
	set service-profile mesh on page 450
	set service-profile bridging on page 437
	display ap boot-configuration on page 342
	display ap mesh-links on page 329

**clear ap
local-switching
vlan-profile**

Clears the VLAN profile that had been applied to an MAP to use with local switching.

Syntax — `clear {ap ap-number local-switching vlan-profile`

- *ap-number* — Index value that identifies the MAP on the WX switch.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.0.

History — A VLAN profile consists of a list of VLANs and tags. When a VLAN profile is applied to a MAP, traffic for the VLANs specified in the VLAN profile is locally switched by the MAP instead of being tunneled back to a WX. When the VLAN profile is cleared from the MAP, traffic that had been locally switched is tunneled to a WX.

When clearing a VLAN profile causes traffic that had been locally switched by MAPs to be tunneled to a WX, the sessions of clients associated with the MAPs where the VLAN profile is applied are terminated, and the clients must re-associate with the MAPs.

Examples — The following command clears the VLAN profile that had been applied to MAP 7:

```
WX# clear ap 7 local-switching vlan-profile
success: change accepted.
```

See Also

- **set vlan profile** on page 127
- **set ap local-switching mode** on page 379
- **set ap local-switching vlan-profile** on page 380

clear ap radio

Disables a MAP radio and resets it to its factory default settings.

Syntax — `clear ap ap-num } radio {1 | 2 | all}`

- **ap *ap-number*** — Index value that identifies the MAP on the WX.
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- **radio all** — All radios on the MAP.

Defaults — The **clear ap radio** command resets the radio to the default settings listed in Table 51 and in Table 72 on page 416.

Table 51 Radio-Specific Parameters

Parameter	Default Value	Description
antennatype	For most MAP models, the default is internal . For MP-620, the default for the 802.11b/g radio is ANT-1360-OUT . The default for the 802.11a radio is ANT-5360 OUT . The default for the 802.11b/g radio on model AP3150 is ANT1060 .	External antenna model Note: This parameter is configurable only on MAPs that support external antennas.
auto-tune	<ul style="list-style-type: none"> ▪ max-power—highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower ▪ max-retransmissions—10 percent ▪ min-client-rate—5.5 Mbps for 802.11b/g; 24 Mbps for 802.11b/g 	<ul style="list-style-type: none"> ▪ RF Auto-Tuning settings: ▪ max-power—maximum power that RF Auto-Tuning can set on a radio ▪ max-retransmissions—maximum percentage of client retransmissions a radio can experience before RF Auto-Tuning considers changing the channel on the radio ▪ min-client-rate—minimum rate at which a radio is allowed to transmit traffic to clients

Table 51 Radio-Specific Parameters (continued)

channel	<ul style="list-style-type: none"> ■ 802.11b — 6 ■ 802.11a — Lowest valid channel number for the country of operation 	Number of the channel in which a radio transmits and receives traffic
mode	<ul style="list-style-type: none"> ■ disable 	Operational state of the radio.
radio-profile	None. You must add the radios to a radio profile.	802.11 settings
tx-power	Highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.	Transmit power of a radio, in decibels referred to 1 milliwatt (dBm)

Access — Enabled

History — Introduced in MSS Version 3.0. Version 6.0 removed the **dap** option for distributed MAPs.

Usage — When you clear a radio, MSS performs the following actions:

- Clears the transmit power, channel, and external antenna setting from the radio.
- Removes the radio from its radio profile and places the radio in the *default* radio profile.

This command does not affect the PoE setting.

Examples — The following command disables and resets radio 2 on the MAP access point connected to port 3:

```
WX1200# clear ap 3 radio 2
```

See Also

- **set ap radio mode** on page 391
- **set ap radio radio-profile** on page 392
- **set port type ap** on page 97

**clear ap
boot-configuration**

Removes the static IP address configuration for a Distributed MAP.

Syntax — `clear ap boot-configuration apnum`

- `ap ap-number` — Index value that identifies the MAP on the WX.

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.2. Version 6.0 removed the **dap** option.

Usage — When the static IP configuration is cleared for a MAP, and a MAP is rebooted, it uses the standard boot process.

Examples — The following command clears the static IP address configuration for MAP 1.

```
WX# clear ap 1 boot-configuration
This will clear specified AP devices. Would you like to
continue? (y/n) [n]y
success: change accepted.
```

See Also

- **display ap boot-configuration** on page 342
- **set ap boot-configuration ip** on page 369
- **set ap boot-configuration switch** on page 374
- **set ap boot-configuration ip** on page 369
- **set ap boot-configuration vlan** on page 375

clear ap radio load-balancing group

Removes a MAP radio from its load-balancing group.

Syntax `clear ap ap-number radio {1 | 2} load-balancing group`

- **ap** *ap-number* — Index value that identifies the MAP on the WX.
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — If an MAP radio has been assigned to an RF load balancing group, you can use this command to remove the MAP radio from the group.

Examples — The following command clears radio 1 on MAP 7 from the load balancing group to which it had been assigned:

```
WX# clear ap 7 radio 1 load-balancing group
WX#
```

See Also

- **display load-balancing group** on page 348
- **set ap radio load balancing on page 389**
- **set load-balancing strictness** on page 399
- **set ap local-switching mode** on page 379

clear radio-profile

Removes a radio profile or resets one of the profile's parameters to its default value.

Syntax — `clear radio-profile name [parameter]`

- *name* — Radio profile name.
- *parameter* — Radio profile parameter:
 - `beacon-interval`
 - `countermeasures`
 - `dtim-interval`
 - `frag-threshold`
 - `max-rx-lifetime`
 - `max-tx-lifetime`
 - `preamble-length`
 - `rts-threshold`
 - `service-profile`

For information about these parameters, see the **set radio-profile** commands that use them.

Defaults — If you reset an individual parameter, the parameter is returned to the default value listed in Table 72 on page 416.

Access — Enabled.

History — Introduced in MSS Version 3.0. **countermeasure** parameter added in Version 4.1. Version 4.2 removes the **long-retry** and **short-retry** parameters that no longer apply to radio profiles.

Usage — If you specify a parameter, the setting is reset to its default value. The settings of the other parameters are unchanged and the radio profile remains in the configuration. If you do not specify a parameter, the entire radio profile is deleted from the configuration. All radios that use this profile must be disabled before you can delete the profile.

Examples — The following commands disable the radios using radio profile *rp1* and reset the **beaconed-interval** parameter to its default value:

```
WX4400# set radio-profile rp1 mode disable
WX4400# clear radio-profile rp1 beacon-interval
success: change accepted.
```


The following commands disable the radios using radio profile *rptest* and remove the profile:

```
WX4400# set radio-profile rptest mode disable
WX4400# clear radio-profile rptest
success: change accepted.
```

See Also

- **display radio-profile** on page 350
- **set ap radio radio-profile** on page 392
- **set radio-profile mode** on page 416
- **display radio-profile** on page 350

clear service-profile

Removes a service profile or resets one of the profile's parameters to its default value.

Syntax — `clear service-profile name`

[`soda {agent-directory | failure-page | remediation-acl | success-page | logout-page}`]

- **soda agent-directory** — Resets the directory for Sygate On-Demand (SODA) agent files to the default directory. By default, the directory name for SODA agent files is the same as the service profile name.
- **soda failure-page** — Resets the page that is loaded when a client fails the SODA agent checks. By default, the page is generated dynamically.
- **soda remediation-acl** — Disables use of the specified remediation ACL for the service profile. When no remediation ACL is specified, a client is disconnected from the network when it fails SODA agent checks.
- **soda success-page** — Resets the page loaded when a client passes the checks performed by the SODA agent. By default, the page is generated dynamically.
- **soda logout-page** — Resets the page loaded when a client logs out of the network. By default, the client is disconnected from the network without loading a page.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. Options added to clear SODA parameters in Version 4.2.

Usage — If the service profile is mapped to a radio profile, you must remove it from the radio profile first. (After disabling all radios that use the radio profile, use the **clear radio-profile** *name* **service-profile** *name* command.)

Examples — The following commands disable the radios using radio profile *rp6*, remove service-profile *svcprof6* from *rp6*, then clear *svcprof6* from the configuration.

```
WX4400# set radio-profile rp6 mode disable
WX4400# clear radio-profile rp6 service-profile svcprof6
success: change accepted.
WX4400# clear service-profile svcprof6
success: change accepted.
```

See Also

- **clear radio-profile** on page 312
- **display service-profile** on page 353
- **set radio-profile mode** on page 416

display ap arp

Displays the ARP table for a specified MAP.

Syntax — **display ap arp** *ap-number*

- *ap-number* — Index value that identifies the MAP on the WX.

Defaults — None.

Access — All.

History — Introduced in MSS Version 6.0.

Examples — The following command displays ARP entries for AP 7:

```
WX# display ap arp 7
```

```
AP 7:
```

Host	HW Address	VLAN	State	Type
10.5.4.51	00:0b:0e:00:04:0c	1	EXPIRED	DYNAMIC
10.5.4.53	00:0b:0e:02:76:f7	1	RESOLVED	LOCAL

Table 52 describes the fields in this display.

Table 52 Output for display ap arp

Field	Description
Host	IP address, hostname, or alias.
HW Address	MAC address mapped to the IP address, hostname, or alias.
VLAN	MAC address mapped to the IP address, hostname, or alias.
State	Entry state: <ul style="list-style-type: none"> RESOLVING—MSS sent an ARP request for the entry and is waiting for the reply. RESOLVED—Entry is resolved. EXPIRED—Entry is expired.
Type	Entry type: <ul style="list-style-type: none"> DYNAMIC—Entry was learned from network traffic and ages out if unused for longer than the ARP aging timeout. LOCAL—Entry for the WX MAC address. Each VLAN has one local entry for the switch MAC address. PERMANENT—Entry does not age out and remains in the configuration even following a reboot. STATIC—Entry does not age out but is removed after a reboot.

See Also

- set ap local-switching mode on page 379
- set vlan profile on page 127

display ap config

Displays global and radio-specific settings for a MAP access point.

Syntax — `display ap config [port-list [radio {1 | 2}]]`

- *ap-number* — Index value that identifies the MAP on the WX.
- **radio 1** — Shows configuration information for radio 1.
- **radio 2** — Shows configuration information for radio 2. (This option does not apply to single-radio models.)

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0. Version 6.0 removed the **dap** option. Version 6.0 also added **Field communication timeout**, **Field load-balance-enable**, **Field force-rebalance**, **Field local-switching**, and **Field vlan-profile**.

Usage — MSS lists information separately for each MAP access point.

Examples — The following example shows configuration information for MAP 2:

```
WX# display ap config 2
AP 2: serial-id: 123456789, AP model: MP-372, bias: high, name: AP02
      upgrade-firmware: YES
      force-image-download: NO
      communication timeout: 10
      location:
      contact:
Radio 1: type: 802.11g, mode: disabled, channel: dynamic
tx pwr: 18, profile: default
auto-tune max-power: default,
load-balance-group: ,
load-balance-enable: YES,
force-rebalance: NO,
local-switching: disabled, vlan-profile: default
```

Table 53 describes the fields in this display.

Table 53 Output for display ap config

Field	Description
Port	WX port number to which the MAP is connected, if specified for the MAP.
AP	Index number that identifies the MAP to the WX.
Serial-Id	Serial ID of the MAP access point.
AP model	MAP access point model number.
bias	Bias of the WX connection to the MAP: <ul style="list-style-type: none"> ▪ High ▪ Low
name	MAP access point name, if configured.
upgrade-firmware	State of the firmware upgrade option: <ul style="list-style-type: none"> ▪ YES (automatic upgrades are enabled) ▪ NO (automatic upgrades are disabled)
force-image-download	State of the option to force the MAP to download its software image from the WX switch instead of loading the image that is locally stored on the MAP.
communication timeout	
location	Location information for the MAP.
contact	Contact information for the MAP.
Radio	Radio number. The information listed below this field applies specifically to the radio.
type	Radio type: <ul style="list-style-type: none"> ▪ 802.11a ▪ 802.11b ▪ 802.11g
mode	Radio state: <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled
channel	Channel number.
antennatype	External antenna model, if applicable.
tx pwr	Transmit power, in dBm.

Table 53 Output for display ap config (continued)

Field	Description
profile	Radio profile that manages the radio. Until you assign the radio to a radio profile, MSS assigns the radio to the default radio profile.
auto-tune max-power	Maximum power level the RF Auto-Tuning feature can set on the radio. <ul style="list-style-type: none"> ▪ The value <i>default</i> means RF Auto-Tuning can set the power up to the maximum level allowed for the country of operation. ▪ A specific numeric value means you or another administrator set the maximum value.
load-balance-group	Names of the RF load-balancing groups to which the MAP access point belongs. If the value is <i>None</i> , the access point does not belong to any load balancing groups. <p>Note: This field is displayed only if the MAP is a member of a group.</p>
load-balance-enable	Whether RF load balancing is enabled for this MAP.
force-rebalance	Whether the MAP radio to disassociates its client sessions and rebalance them whenever a new MAP radio is added to the RF load balancing group.
local-switching	Whether local packet switching is enabled for the MAP.
vlan-profile	The VLAN profile the MAP uses for local packet switching, indicating which VLANs are locally switched.

See Also

- **display ap connection** on page 343
- **display ap global** on page 345
- **display ap unconfigured** on page 347
- **display radio-profile** on page 350
- **set ap** on page 87
- **set port type ap** on page 97
- **set ap bias** on page 367
- **set ap group** on page 379
- **set ap name** on page 381
- **set ap upgrade-firmware** on page 396

- **set ap radio mode** on page 391
- **set ap radio antennatype** on page 383
- **set ap radio channel** on page 387
- **set ap radio radio-profile** on page 392
- **set ap radio tx-power** on page 393

display ap counters Displays MAP access point and radio statistics counters.

Syntax — `display ap counters [ap-number[radio {1 | 2}]]`

- *ap-number* — Index value that identifies the MAP on the WX.
- **radio 1** — Shows statistics counters for radio 1.
- **radio 2** — Shows statistics counters for radio 2. (This option does not apply to single-radio models.)

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0. New fields added in MSS Version 4.0:

- Radio Recv Phy Err Ct
- Transmit Retries
- Radio Adjusted Tx Pwr
- Noise Floor
- 802.3 Packet Tx Ct
- 803.3 Packet Rx Ct
- No Receive Descriptor

Version 6.0 removed the **dap** option and added the Illegal Rates field.

Usage — To display statistics counters and other information for individual user sessions, use the **display sessions network** command.

Examples — The following command shows statistics counters for Distributed MAP 7:

```
WX1200# display ap counters 7
AP: 7          radio: 1
=====
LastPktXferRate      2          PktTxCount          91594255
NumCntInPwrSave     4294966683MultiPktDrop      0
LastPktRxSigStrength -54          MultiBytDrop        0
LastPktSigNoiseRatio 40          User Sessions       5
TKIP Pkt Transfer Ct 0           MIC Error Ct        0
TKIP Pkt Replays    0           TKIP Decrypt Err    0
CCMP Pkt Decrypt Err 0           CCMP Pkt Replays    0
CCMP Pkt Transfer Ct 0           RadioResets         0
Radio Recv Phy Err Ct 0           Transmit Retries    60501
Radio Adjusted Tx Pwr 15          Noise Floor         -93
802.3 Packet Tx Ct  0           802.3 Packet Rx Ct 0
No Receive Descriptor 0           Illegal Rates       2
```

	TxUniPkt	TxUniByte	RxPkt	RxByte	UndcrptPkt	UndcrptByte	PhyError		
	TxMultiPkt	TxMultiByte							
1.0:	164492	0	9631741	0	405041	8913512	0	0	13963
2.0:	603	0	248716	0	191103	4608065	0	0	30547
5.5:	370594	52742	27616521	4445625	2427	133217	0	0	723
6.0:	0	0	0	0	0	0	0	0	51
9.0:	0	0	0	0	1	172	0	0	53
11.0:	8016	0	2590353	0	85479	3897587	0	0	1195
12.0:	0	0	0	0	0	0	0	0	26
18.0:	0	0	0	0	0	0	0	0	38
24.0:	0	0	0	0	0	0	0	0	47
36.0:	0	0	0	0	0	0	0	0	1
48.0:	0	0	0	0	1	68	0	0	29
54.0:	0	0	0	0	0	0	0	0	5
TOTL:	543705	52742	40087331	4445625	684050	17552381	0	0	46441

Table 54 describes the fields in this display.

Table 54 Output for display ap counters

Field	Description
AP	Distributed MAP number.
Port	WX port number (if the MAP is directly connected to the WX and the WX port is configured as a MAP access point).
radio	Radio number.
LastPktXferRate	Data transmit rate, in Mbps, of the last packet received by the MAP access point.
NumCntlnPwrSave	Number of clients currently in power save mode.
LastPktRxSigStrength	Signal strength, in dBm, of the last packet received by the MAP access point.
LastPktSigNoiseRatio	<p>Signal-to-noise ratio, in decibels (dB), of the last packet received by the MAP access point.</p> <p>This value indicates the strength of the radio signal above the noise floor. For example, if the noise floor is -88 and the signal strength is -68, the SNR is 20.</p> <p>If the value is below 10, this indicates a weak signal and might indicate a problem in the RF environment.</p>
TKIP Pkt Transfer Ct	Total number of TKIP packets sent and received by the radio.
TKIP Pkt Replays	<p>Number of TKIP packets that were resent to the MAP by a client.</p> <p>A low value (under about one hundred) does not necessarily indicate a problem. However, if this counter is increasing steadily or has a very high value (in the hundreds or more), a Denial of Service (DoS) attack might be occurring. Contact 3Com TAC.</p>
CCMP Pkt Decrypt Err	<p>Number of times a decryption error occurred with a packet encrypted with CCMP.</p> <p>Occasional decryption errors do not indicate a problem.</p> <p>However, steadily increasing errors or a high number of errors can indicate that data loss is occurring in the network. Generally, this is caused by a key mismatch between a client and the MAP. To locate the client that is experiencing decryption errors (and therefore is likely causing this counter to increment on the MAP), use the display sessions network session-id session-id command for each client on the radio. After you identify the client that is causing the errors, disable and reenble the client (wireless NIC).</p>

Table 54 Output for display ap counters (continued)

Field	Description
CCMP Pkt Transfer Ct	Total number of CCMP packets sent and received by the radio.
Radio Recv Phy Err Ct	Number of times radar caused packet errors. If this counter increments rapidly, there is a problem in the RF environment. This counter increments only when radar is detected. Rate-specific Phy errors are instead counted in the PhyError columns for individual data rates.
Radio Adjusted Tx Pwr	Current power level set on the radio. If RF Auto-Tuning of power is enabled, this value is the power set by RF Auto-Tuning. If RF Auto-Tuning is disabled, this value is the statically configured power level.
802.3 Packet Tx Ct	Number of raw 802.3 packets transmitted by the radio. These are LocalTalk (AppleTalk) frames. This counter increments only if LocalTalk traffic is present.
No Receive Descriptor	Number of packets for which the MAP could not create a descriptor. A descriptor describes a received packet's size and its location in MAP memory. The MAP buffers descriptors, and clears them during interframe spaces. This counter increments if the MAP runs out of buffers for received packets. This condition can occur when a noise burst temporarily floods the air and the MAP attempts to buffer the noise as packets. Buffer overruns are normal while a MAP is booting. However, if they occur over an extended period of time when the MAP is fully active, this can indicate RF interference.
Illegal Rates	Number of times a client attempted to connect with a disabled data rate.
PktTxCount	Number of packets transmitted by the radio.
MultiPktDrop	Number of multicast packets dropped by the radio due to a buffer overflow on the MAP. This counter increments if there is too much multicast traffic or there is a problem with the multicast packets. Normally, this counter should be 0.
MultiBytDrop	Number of multicast bytes dropped by the radio due to a buffer overflow on the MAP. (See the description for MultiPktDrop.)

Table 54 Output for display ap counters (continued)

Field	Description
User Sessions	<p>Number of clients currently associated with the radio.</p> <p>Generally, this counter is equal to the number of sessions listed for the radio in display sessions output. However, the counter can differ from the counter in display sessions output if a client is associated with the radio but has not yet completed 802.1X authentication. In this case, the client is counted by this counter but not in the display sessions output.</p> <p>Although there is no specific normal range for this counter, a high or low number relative to other radios can mean the radio is underutilized or overutilized relative to the other radios. (However, if the clients are VoIP phones, a relatively high number of clients does not necessarily mean overutilization since voice clients consume less bandwidth on average than data clients.)</p>
MIC Error Ct	<p>Number of times the radio received a TKIP-encrypted frame with an invalid MIC.</p> <p>Normally, the value of this counter should always be 0. If the value is not 0, check the system log for MIC error messages and contact 3Com TAC.</p>
TKIP Decrypt Err	<p>Number of times a decryption error occurred with a packet encrypted with TKIP.</p> <p>(See the description for CCMP Pkt Decrypt Err.)</p>
CCMP Pkt Replays	<p>Number of CCMP packets that were resent to the MAP by a client.</p> <p>(See the description for TKIP Pkt Replays.)</p>
RadioResets	<p>Number of times the radio has been reset. Generally, a reset occurs as a result of RF noise. It is normal for this counter to increment a few times per day.</p>
Transmit Retries	<p>Number of times the radio retransmitted a unicast packet because it was not acknowledged. The MAP uses this counter to adjust the transmit data rate for a client, in order to minimize retries.</p> <p>The ratio of transmit retries to transmitted packets (TxUniPkt) indicates the overall transmit quality. A ratio of about 1 retry to 10 transmitted packets indicates good transmit quality. A ratio of 3 or more to 10 indicates poor transmit quality.</p> <p>This counter includes unacknowledged probes. Some clients do not respond to probes, which can make this counter artificially high.</p>

Table 54 Output for display ap counters (continued)

Field	Description
Noise Floor	Received signal strength at which the MAP can no longer distinguish 802.11 packets from ambient RF noise. A value around -90 or higher is good for an 802.11b/g radio. A value around -80 or higher is good for an 802.11a radio. Values near 0 can indicate RF interference.
802.3 Packet Rx Ct	Number of raw 802.3 packets received by the radio. These are LocalTalk (AppleTalk) frames. This counter increments only if LocalTalk traffic is present.
<p>The counters above are global for all data rates. The counters below are for individual data rates.</p> <p>If counters for lower data rates are incrementing but counters for higher data rates are not incrementing, this can indicate poor throughput. The poor throughput can be caused by interference. If the cause is not interference or the interference cannot be eliminated, you might need to relocate the MAP in order to use the higher data rates and therefore improve throughput.</p>	
TxUniPkt	Number of unicast packets transmitted by the radio..
TxMultiPkt	Number of multicast packets transmitted by the radio.
TxUniByte	Number of unicast bytes transmitted by the radio.
TxMultiByte	Number of multicast bytes transmitted by the radio.
RxPkt	Number of packets received by the radio.
RxByte	Number of bytes received by the radio.
UndcrptPkt	Number of undecryptable packets received by the radio. It is normal for this counter to increment even in stable networks and does not necessarily indicate an attack. For example, a client might be sending incorrect key information. However, if the counter increments rapidly, there might be a problem in the network.
UndcrptByte	Number of undecryptable bytes received by the radio. (See the description for UndcrptPkt.)
PhyError	<p>Number of packets that could not be decoded by the MAP. This condition can have any of the following causes:</p> <ul style="list-style-type: none"> ■ Collision of an 802.11 packet. ■ Packet whose source is too far away, thus rendering the packet unintelligible by the time it reaches the MAP. ■ Interference caused by an 802.11b/g phone or other source. <p>It is normal for this counter to be about 10 percent of the total RxByte count. It is also normal for higher data rates to have higher Phy error counts than lower data rates.</p>

See Also

- **display sessions network** on page 620

display ap fdb

Displays the entries in a specified MP's forwarding database.

Syntax — `display ap fdb ap-number`

- *ap-number* — Index value that identifies the MAP on the WX.

Defaults — None.

Access — All.

History — Introduced in MSS Version 6.0.

Examples — The following command displays FDB entries for AP 7:

```
WX# display ap fdb 7
AP 7:
# = System Entry. $ = Authenticate Entry
VLAN    TAG    Dest MAC/Route Des [CoS]    Destination Ports
-----  ---    -
4095    4095    00:0b:0e:00:ca:c1    #    CPU
4095    0       00:0b:0e:00:04:0c        eth0
```

Table 55 describes the fields in the **display ap fdb** output.

Table 55 Output for display ap fdb

Field	Description
VLAN	VLAN number.
TAG	VLAN tag value. If the interface is untagged, the TAG field is blank.
Dest MAC/Route Des	MAC address of this forwarding entry's destination.
CoS	Type of entry. The entry types are explained in the first row of the command output. Note: This Class of Service (CoS) value is not associated with MSS quality of service (QoS) features.
Destination Ports	WX switch port associated with the entry. A switch sends traffic to the destination MAC address through this port.

See Also

- **set ap local-switching mode** on page 379
- **set vlan profile** on page 127

display ap qos-stats Displays statistics for MAP forwarding queues.

Syntax — `display ap qos-stats [ap-number][clear]`

- *ap-number* — Index value that identifies the MAP on the WX.
- **clear** — Clears the counters after displaying their current values.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0. Version 4.2 added the TxDrop field. Version 6.0 removed the **dap** option.

Usage — Repeating this command with the **clear** option at regular intervals allows you to monitor transmission and drop rates.

Examples — The following command shows statistics for the MAP forwarding queues on a Distributed MAP.

```
WX4400# display ap qos-stats 4
CoS   Queue           Tx           TxDrop
=====
      AP: 4 radio: 1
1,2   Background       0            0
0,3   BestEffort       15327        278
4,5   Video            0            0
6,7   Voice            1714881      0
      AP: 4 radio: 2
1,2   Background       0            0
0,3   BestEffort       0            0
4,5   Video            0            0
6,7   Voice            0            0
```

Table 56 describes the fields in this display.

Table 56 Output for display ap qos-stats

Field	Description
CoS	CoS value associated with the forwarding queues.
Queue	Forwarding queue.
AP	Distributed MAP number or MAP port number.
radio	Radio number.
Tx	Number of packets transmitted to the air from the queue.
TxDrop	Number of packets dropped from the queue instead of being transmitted. Some packet drops are normal, especially if the RF environment is <i>noisy</i> . Also, it is normal for a mildly congested radio to drop low-priority packets proportionally more often than high-priority packets. However, continuous packet drops from the Voice queue can indicate over-subscription or excessive interference in the RF environment.

display ap etherstats

Displays Ethernet statistics for an Ethernet port on a MAP.

Syntax — `display ap etherstats ap-number`

- *ap-number* — Index value that identifies the MAP on the WX.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command displays Ethernet statistics for the Ethernet ports on Distributed MAP 1:

```
WX4400# display ap etherstats 1
AP: 1 ether: 1
=====
RxUnicast:          75432 TxGoodFrames:          55210
RxMulticast:        18789 TxSingleColl:           32
RxBroadcast:         8 TxLateColl:            0
RxGoodFrames:       94229 TxMaxColl:            0
RxAlignErrs:         0 TxMultiColl:           47
RxShortFrames:       0 TxUnderruns:           0
RxCrcErrors:         0 TxCarrierLoss:          0
RxOverruns:          0 TxDeferred:            150
RxDiscards:          0
```

Table 57 describes the fields in this display.

Table 57 Output of display ap etherstats

Field	Description
RxUnicast	Number of unicast frames received.
RxMulticast	Number of multicast frames received.
RxBroadcast	Number of broadcast frames received.
RxGoodFrames	Number of frames received properly from the link.
RxAlignErrs	Number of received frames that were both misaligned and contained a CRC error.
RxShortFrames	Number of received frames that were shorter than the minimum frame length.
RxCrcErrors	Number of received frames that were discarded due to CRC errors.
RxOverruns	Number of frames known to be lost due to a temporary lack of hardware resources.
RxDiscards	Number of frames known to be lost due to a temporary lack of software resources.
TxGoodFrames	Number of frames transmitted properly on the link.
TxSingleColl	Number of transmitted frames that encountered a single collision.
TxLateColl	Number of frames that were not transmitted because they encountered a collision outside the normal collision window.

Table 57 Output of display ap etherstats (continued)

Field	Description
TxMaxColl	Number of frames that were not transmitted because they encountered the maximum allowed number of collisions. Typically, this occurs only during periods of heavy traffic on the network.
TxMultiColl	Number of transmitted frames that encountered more than one collision.
TxUnderruns	Number of frames that were not transmitted or retransmitted due to temporary lack of hardware resources.
TxCARRIERLoss	Number of frames transmitted despite the detection of a deassertion of CRS during the transmission.
TxDeferred	Number of frames deferred before transmission due to activity on the link.

display ap group

Deprecated in MSS Version 6.0. To display information about RF load balancing, see “display load-balancing group” on page 348.

display ap mesh-links

Displays information about the links an MAP has to Mesh APs and Mesh Portal APs.

Syntax — **display ap mesh-links** *ap-number* [*path*]

- *ap-number* — Index value that identifies the MAP on the WX.
- *path* — Displays statistics for the path of mesh services devices of which this MAP is part.

Defaults — None.

Access — All.

History — Introduced in MSS Version 6.0.

Examples — The following command mesh link information for AP 7:

```
WX# display ap mesh-links 7
AP: 7 IP-addr: 1.1.1.3
Operational Mode: Mesh-Portal
Downlink Mesh-APs
-----
BSSID: 00:0b:0e:17:bb:3f (54 Mbps)
      packets          bytes
TX:           307      44279
RX:           315      215046
```

The following command displays statistics for the path of mesh services devices that MAP is part of.

```
WX# display ap mesh-links 7 path
Status Flags:
m - Mesh AP, p - Mesh Portal, b - Bridging
AP  Current Uplink Uplink Uplink  Packets
Num Status  AP      RSN    RX     TX
-----
0007 ----      -
```

Table 58 describes the fields in the **display ap mesh-links** output.

Table 58 Output for display ap mesh-links

Field	Description
AP	Identifier for the MAP on the WX switch.
Name	VLAN name
IP-addr	IP address of the MAP.
Operational Mode	Whether this MAP is a Mesh AP or a Mesh Portal AP Downlink Mesh-APs Information about the Mesh APs for which this MAP is a Mesh Portal MAP.
Downlink Mess-APs	Information about the Mesh APs for which this MAP is a Mesh Portal MAP.
BSSID	The BSSID of the Mesh AP.
TX	The amount of traffic (packets and bytes) transmitted to the Mesh AP.
RX	The amount of traffic (packets and bytes) received from the Mesh AP.

See Also

- **set ap boot-configuration mesh ssid** on page 373
- **set service-profile mesh** on page 450

display ap status

Displays MAP access point and radio status information.

Syntax — `display ap status [terse] [ap-number | all [radio {1 | 2}]]`

- **terse** — Displays a brief line of essential status information for each MAP.
- *ap-number* — Index value that identifies the MAP on the WX.
- **all** — Shows status information for all directly attached MAP access points and all Distributed MAP access points configured on the switch.
- **radio 1** — Shows status information for radio 1.
- **radio 2** — Shows status information for radio 2. (This option does not apply to single-radio models.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. True base MAC addresses of radios are displayed in MSS Version 3.2. Previously, the base MAC address displayed for a radio was the true base MAC address plus 2. Note that a radio's base MAC address is also used as the BSSID of the first SSID configured on the radio. New option added: **terse**; new option added for **display ap status: all**; new field added: **fingerprint**; MAP-WX security status added to **State** field in MSS Version 4.0. External antenna information added after the radio state information, to indicate when an antenna has been detected and to indicate the configured antenna model number; *auto* flag added to indicate operational channel or power settings that are configured by RF Auto-Tuning in MSS Version 4.1. Version 4.2 added *Radar Scan and Radar Detected* flags to indicate when the Dynamic Frequency Selection (DFS) feature is scanning for radar or has stopped transmitting due to detected radar. The flags apply to 802.11a radios only, and only for country codes where DFS is used.

Version 6.0 removed the **dap** option.

Examples — The following command displays the status of a MAP access point:

```
WX4400# display ap status 7
Dap: 1, IP-addr: 10.2.34.56 (vlan 'vlan-corp'), MAP model: AP2750,
      manufacturer: 3Com, name: DAP01
      fingerprint: b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3
=====
State:      operational
CPU info:   IBM:PPC speed=266666664 Hz version=405GPr
            id=0x28f10158a47f0408 ram=33554432
            s/n=0332600444 hw_rev=A3
Uptime:    21 hours, 27 minutes, 51 seconds

Radio 1 type: 802.11g, state: configure succeed [Enabled]
operational channel: 64 operational power: 14
base mac: 00:0b:0e:00:d2:c1
bssid1: 00:0b:0e:00:d2:94, ssid: private
```

The following command displays the status of a directly connected MAP:

```
WX# display ap status 7
AP: 7, AP model: MP-252, manufacturer 3Com, name: MP07
=====
State: operational (not encrypt)
CPU info: IBM:PPC speed=266666664 Hz version=405GPr, ram=33554432
s/n=0333703050 hw_rev=A3
Uptime: 503 hours, 51 minutes, 5 seconds
Radio 1 type: 802.11g, state: configure succeed [Enabled]
operational channel: 11 (Auto) operational power: 1
bssid1: 00:0b:0e:00:ca:c0, ssid: public
bssid2: 00:0b:0e:00:ca:c2, ssid: employee-net
load balance: enabled, current load: (unavailable)
RFID Reports: Inactive
Radio 2 type: 802.11a, state: configure succeed [Disabled] (Sweep mode)
operational channel: 44 (Auto) operational power: 1
bssid1: 00:0b:0e:00:ca:c1, ssid: mycorp-tkip
load balance: enabled, current load: (unavailable)
RFID Reports: Inactive
```

The following command uses the **terse** option to display brief information for MAPs:

```
WX# display ap status terse
Total number of entries: 120
Operational: 1, Image Downloading: 0, Unknown: 119, Other: 0
Flags: o = operational, b = booting, d = image downloading
       c = configuring, f = configuration failed
       a = auto AP, m = mesh AP, p = mesh portal
       i = insecure, e = encrypted, u = unencrypt
AP  Flag IP Address          Model    MAC Address          Radio1 Radio2 Uptime
---  ---  -
 7  o--u                    MP-252   00:0b:0e:00:ca:c0   D11/1  D44/1  21d00h
```

Table 59 and Table 60 describe the fields in this display.

Table 59 Output for display ap status

Field	Description
AP	Connection ID for the Distributed MAP. Note: This field is applicable only if the MAP is configured on the WX switch as a Distributed MAP.
Port	WX port number. Note: This field is applicable only if the MAP is directly connected to the WX switch and the WX switch port is configured as a MAP access port.
IP-addr	IP address of the MAP. The address is assigned to the MAP by a DHCP server. Note: This field is applicable only if the MAP is not directly attached to the WX switch.
AP model	MAP access point model number.
manufacturer	Company that made the MAP access point.
fingerprint	Hexadecimal fingerprint of the MAP's public encryption key. Note: This field is displayed only if the MAP is not directly attached to the WX switch.
name	MAP access point name.
Link	Status of this link with the MAP access point and the MAP port at the other end of the link. The status can be up or down.
MAP port	MAP port number connected to this WX port.

Table 59 Output for display ap status (continued)

Field	Description
State	<p data-bbox="658 305 843 331">State of the MAP:</p> <ul style="list-style-type: none"> <li data-bbox="658 348 1283 401">■ init — The MAP has been recognized by the WX but has not yet begun booting. <li data-bbox="658 418 1283 470">■ booting — The MAP has asked the WX for a boot image. <li data-bbox="658 487 1283 539">■ image downloading — The MAP is receiving a boot image from the WX. <li data-bbox="658 557 1283 609">■ image downloaded — The MAP has received a boot image from the WX and is booting. <li data-bbox="658 626 1283 678">■ configuring — The MAP has booted and is ready to receive or is already receiving configuration parameters from the WX. <li data-bbox="658 696 1283 782">■ operational — The MAP has received configuration parameters for one or more radios and is ready to accept client connections. <li data-bbox="658 800 1283 852">■ configure failure — One or more of the radio parameters received from the WX is invalid. <p data-bbox="658 869 1283 947">For Distributed MAPs, this field also indicates whether the MAP management traffic with the WX is encrypted, and whether the MAP's fingerprint has been verified on the WX:</p> <ul style="list-style-type: none"> <li data-bbox="658 965 1283 1017">■ not encrypted—The management session is not encrypted. <li data-bbox="658 1034 1283 1112">■ encrypted but fingerprint not verified—The MAP management traffic is encrypted, but the MAP fingerprint has not been verified in MSS. <li data-bbox="658 1130 1283 1199">■ encrypted and verified—The MAP management traffic is encrypted and the MAP fingerprint has been verified in MSS.
CPU info	<p data-bbox="658 1216 1108 1242">Specifications and identification of the CPU.</p> <p data-bbox="658 1260 1283 1312">For MAP models MP-352, MP-341, and MP-52, the ID portion of this field is not applicable.</p>
Uptime	<p data-bbox="658 1329 1283 1355">Amount of time since the MAP last rebooted using this link.</p> <p data-bbox="658 1373 1283 1421">Note: This field is displayed only when this link is the MAP access point's primary link.</p>

Table 59 Output for display ap status (continued)

Field	Description
Radio 1 type	802.11 type and configuration state of the radio.
Radio 2 type	<ul style="list-style-type: none"> ■ The <i>configure succeed</i> state indicates that the MAP has received configuration parameters for the radio and the radio is ready to accept client connections. ■ <i>802.11b protect</i> indicates that the 802.11b/g radio is sending messages to 802.11b devices, while sending 802.11g traffic at higher data rates, to inform the 802.11b devices about the 802.11g traffic and reserve bandwidth for the traffic. Protection mode remains in effect until 60 seconds after the last 802.11b traffic is detected by the 802.11b/g radio. ■ <i>Sweep Mode</i> indicates that a disabled radio is nonetheless participating in rogue detection scans. Even though this message appears only for disabled radios, all radios, enabled or disabled, participate in rogue detection. ■ <i>Countermeasures Enabled</i> indicates that the radio is sending countermeasures packets to combat a rogue. ■ <i>Radar Scan</i> indicates that the radio is performing the initial channel availability check for Dynamic Frequency Selection (DFS). This state lasts during the first 60 seconds an 802.11a radio is on a new channel, during which time the radio does not transmit. If the radio does not detect any radar on the channel, the radio starts using the channel for data. If the radio does detect radar, the flag changes to <i>Radar Detected</i>. (See below). ■ <i>Radar Detected</i> indicates that DFS has detected radar on the channel. When this occurs, the MAP stops transmitting on the channel for 30 minutes. If RF Auto-Tuning is enabled for channel assignment, the radio selects another channel and performs the initial channel availability check on the new channel, during which time the flag changes back to <i>Radar Scan</i>. <p>Note: <i>Radar Scan</i> and <i>Radar Detected</i> apply only to 802.11a radios, for country codes that use DFS.</p>

Table 59 Output for display ap status (continued)

Field	Description
Radio 1 type	<ul style="list-style-type: none"> ■ The following information appears for external antennas: <p><i>External antenna detected, configured as antenna-model</i>—Indicates that an external antenna has been detected, and lists the antenna model configured on the radio. (MSS does not detect the specific model.)</p> <p><i>External antenna detected, not configured</i>—Indicates that an external antenna was detected but no external antenna is configured on the radio.</p> <p><i>External antenna not detected, configured as antenna-model</i>—Indicates that an external antenna is configured on the radio but no external antenna was detected.</p>
Radio 2 type	
(cont.)	
operational channel	The channel on which the radio is currently operating. If the channel number is followed by <i>(Auto)</i> , the value was set by RF Auto-Tuning.
operational power	The power level at which the radio is currently operating. If the power setting is followed by <i>(Auto)</i> , the value was set by RF Auto-Tuning.
base mac	Base MAC address of the radio.
bssid, ssid	SSIDs configured on the radio and their BSSIDs.
load balance	Whether RF load balancing is enabled for the radio.
current load	The load on this radio relative to the load balancing group average or target load.

Table 60 Output for display ap status terse

Field	Description
AP	The number of the MAP connected.
Flag	Operational status flags for the MAP. For flag definitions, see the key in the command output.
Port	WX port number connected to the MAP.
Flg	Operational status flags for the MAP. For flag definitions, see the key in the command output.
IP Address	IP address of the MAP. The address is assigned to the MAP by a DHCP server. This field is applicable only if the MAP is configured on the WX switch as a Distributed MAP.

Table 60 Output for display ap status terse (continued)

Field	Description
Model	MAP model number.
MAC Address	MAC address of the MAP.
Radio1	State, channel, and power information for radio 1: The state can be D (disabled) or E (enabled). The channel and power settings are shown as <i>channel/power</i> .
Radio2	State, channel, and power information for radio 2.
Uptime	Amount of time since the MAP booted using this link.

display ap vlan

Displays information about the VLANs that are either locally switched by the specified MAP or tunneled from the MAP to an WX switch.

Syntax — `display ap vlan ap-number`

- `ap-number` — Index value that identifies the MAP on the WX.

Defaults — None.

Access — All.

History — Introduced in MSS Version 6.0.

Examples — The following command displays information about the VLANs switched by AP 7:

```
WX# display ap vlan 7
AP 7:
VLAN Name           Mode   Port           Tag
-----
  1 default          local
  2 red              local
                        radio_1    20
                        radio_1    21
                        radio_2    22
  4 green            local
                        radio_1    23
  5 yellow           tunnel
                        wx_tun     5
                        radio_1    24
```

Table 61 describes the fields in the **display ap vlan** output.

Table 61 Output for display ap vlan

Field	Description
VLAN	VLAN number.
Name	VLAN name
Mode	Whether packets for the VLAN are locally switched by the MAP, or are tunneled to an WX switch, which places them on the VLAN.
Port	The port(s) through which traffic for the VLAN is sent.
TAG	VLAN tag value. If the interface is untagged, none is displayed in the TAG field.

See Also

- **set ap local-switching mode** on page 379
- **set vlan profile** on page 127

display auto-tune attributes

Displays the current values of the RF attributes RF Auto-Tuning uses to decide whether to change channel or power settings.

Syntax — display auto-tune attributes

```
[ap ap-number [radio {1 | 2 | all}]]
```

- *ap-number* — Index value that identifies the MAP on the WX.
- **radio 1** — Shows RF attribute information for radio 1.
- **radio 2** — Shows RF attribute information for radio 2. (This option does not apply to single-radio models.)
- **radio all** — Shows RF attribute information for both radios.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. Version 6.0 removed the **dap** option.

Examples — The following command displays RF attribute information for radio 1 on the directly connected MAP access point on port 2:

```
WX1200# display auto-tune attributes ap 2 radio 1
Auto-tune attributes for port 2 radio 1:
Noise:                -92 Packet Retransmission Count:      0
Utilization:          0  Phy Errors Count:                  0
CRC Errors count:     122
```

Table 62 describes the fields in this display.

Table 62 Output for display auto-tune attributes

Field	Description
Noise	Noise threshold on the active channel. RF Auto-Tuning prefers channels with low noise levels over channels with higher noise levels.
Utilization	Number of multicast packets per second that a radio can send on a channel while continuously sending fixed size frames over a period of time. The number of packets that are successfully transmitted indicates how busy the channel is.
CRC Errors count	Number of frames received by the radio on that active channel that had CRC errors. A high CRC error count can indicate a hidden node or co-channel interference.
Packet Retransmission Count	Number of retransmitted packets sent from the client to the radio on the active channel. Retransmissions can indicate that the client is not receiving ACKs from the MAP radio.
Phy Errors Count	Number of frames received by the MAP radio that had physical layer errors on the active channel. Phy errors can indicate interference from a non-802.11 device.

See Also

- **display auto-tune neighbors** on page 340
- **display radio-profile** on page 350
- **set ap radio auto-tune max-power** on page 384
- **set ap radio auto-tune max- retransmissions** on page 385
- **set radio-profile auto-tune channel-config** on page 402
- **set radio-profile auto-tune channel-holddown** on page 403
- **set radio-profile auto-tune channel-interval** on page 404
- **set radio-profile auto-tune power-config** on page 406
- **set radio-profile auto-tune power-interval** on page 407

display auto-tune neighbors

Displays the other 3Com radios and third-party 802.11 radios that a 3Com radio can hear.

Syntax — **display auto-tune neighbors**

```
[ap map-num [radio {1 | 2 | all}]]
```

Syntax — **display auto-tune neighbors**

```
[ap ap-number [radio {1 | 2 | all}]]
```

- *ap-number* — Index value that identifies the MAP on the WX.
- **radio 1** — Shows neighbor information for radio 1.
- **radio 2** — Shows neighbor information for radio 2. (This option does not apply to single-radio models.)
- **radio all** — Shows neighbor information for both radios.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. Version 6.0 removed the **dap** option.

Usage — For simplicity, this command displays a single entry for each 3Com radio, even if the radio is supporting multiple BSSIDs. However, BSSIDs for third-party 802.11 radios are listed separately, even if a radio is supporting more than one BSSID.

Information is displayed for a radio if the radio sends beacon frames or responds to probe requests. Even if a radio SSIDs are unadvertised, 3Com radios detect the empty beacon frames (beacon frames without SSIDs) sent by the radio, and include the radio in the neighbor list.

Examples — The following command displays neighbor information for radio 1 on the directly connected MAP access point on port 2:

```
WX1200# display auto-tune neighbors ap 2 radio 1
Total number of entries for port 2 radio 1: 5
Channel Neighbor BSS/MAC  RSSI
-----
1 00:0b:85:06:e3:60  -46
1 00:0b:0e:00:0a:80  -78
1 00:0b:0e:00:d2:c0  -74
1 00:0b:85:06:dd:00  -50
1 00:0b:0e:00:05:c1  -72
```

Table 63 describes the fields in this display.

Table 63 Output for display auto-tune neighbors

Field	Description
Channel	Channel on which the BSSID is detected.
Neighbor BSS/MAC	BSSID detected by the radio.
RSSI	Received signal strength indication (RSSI), in decibels referred to 1 milliwatt (dBm). A higher value indicates a stronger signal.

See Also

- **display auto-tune attributes** on page 338
- **display radio-profile** on page 350
- **set ap radio auto-tune max-power** on page 384
- **set ap radio auto-tune max- retransmissions** on page 385
- **set radio-profile auto-tune channel-config** on page 402
- **set radio-profile auto-tune channel-holddown** on page 403
- **set radio-profile auto-tune channel-interval** on page 404
- **set radio-profile auto-tune power-config** on page 406
- **set radio-profile auto-tune power-interval** on page 407

**display ap
boot-configuration**

Displays information about the static IP address configuration (if any) on a Distributed MAP.

Syntax — `display ap boot-configuration ap-number`

- `ap-number` — Index value that identifies the MAP on the WX.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.2. Version 6.0 removed the **dap** option, and added the following fields.

- Field Mesh
- Field Mesh SSID
- Field Mesh PSK

Examples — The following command displays static IP configuration information for Distributed MAP 1:

```
WX# display ap boot-configuration 1
Static Boot Configuration
AP: 7
IP Address: Disabled
VLAN Tag: Disabled
Switch: Disabled
Mesh: Disabled
IP Address:
Netmask:
Gateway:
VLAN Tag:
Switch IP:
Switch Name:
Mesh SSID:
Mesh PSK:
```

Table 64 describes the fields in this display.

Table 64 Output for display ap boot-configuration

Field	Description
AP	Distributed MAP number.
IP address	Whether static IP address assignment is enabled for this Distributed MAP.
VLAN Tag	Whether the Distributed MAP is configured to use a VLAN tag.
Switch	Whether the Distributed MAP is configured to use a manually specified WX switch as its boot device.
Mesh	Whether WLAN mesh services are enabled for this MAP.
IP address	The static IP address assigned to this Distributed MAP.
Netmask	The subnet mask assigned to this Distributed MAP.
Gateway	The IP address of the default gateway assigned to this Distributed MAP.
VLAN Tag	The VLAN tag that the Distributed MAP is configured to use (if any).
Switch IP	The IP address of the WX switch that this Distributed MAP is configured to use as its boot device (if any).
Switch Name	The name of the WX switch that this Distributed MAP is configured to use as its boot device (if any).
DNS IP	The IP address of the DNS server that the Distributed MAP uses to resolve the name of the WX switch used as its boot device.
Mesh SSID	The WLAN mesh services SSID this MAP is configured to use (if any).
Mesh PSK	The preshared key (PSK) the MAP uses for authentication with a Mesh Portal AP (if any).

display ap connection

Displays the system IP address of the WX switch that booted a Distributed MAP.

Syntax — display ap connection

[*ap-number* | **serial-id** *serial-ID*]

- *ap-number* — Index value that identifies the MAP on the WX.
- **serial-id** *serial-ID* — MAP access point serial ID.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. Version 6.0 removed the **dap** option.

Usage — The **serial-id** parameter displays the active connection for the specified Distributed MAP even if that MAP is not configured on this WX switch. If you instead use the command with the *dap-num* parameter or without a parameter, connection information is displayed only for Distributed MAPs that are configured on this WX switch.

This command provides information only if the Distributed MAP is configured on the switch where you use the command. The switch does not need to be the one that booted the MAP, but it must have the MAP in its configuration. Also, the switch that booted the MAP must be in the same Mobility Domain as the switch where you use the command.

If a Distributed MAP is configured on this WX switch (or another WX switch in the same Mobility Domain) but does not have an active connection, the command does not display information for the MAP. To show connection information for Distributed MAPs, use the **display ap global** command on one of the switches where the MAPs are configured.

Examples — The following command displays information for all Distributed MAPs configured on this WX switch that have active connections:

```
WX1200# display ap connection
Total number of entries: 2
AP Serial Id      AP IP Address    WX IP Address
-----
2   M9DE48B012F00  10.10.2.27      10.3.8.111
4   M9DE48B123400  10.10.3.34      10.3.8.111
```

The following command displays connection information specifically for a Distributed MAP with serial ID *M9DE48B6EAD00*:

```
WX1200# display ap connection serial-id M9DE48B6EAD00
Total number of entries: 1
DAP Serial Id     DAP IP Address    WX IP Address
-----
9   M9DE48B6EAD00  10.10.4.88      10.9.9.11
```

Table 65 describes the fields in this display.

Table 65 Output of display ap connection

Field	Description
AP	ID assigned to the Distributed MAP. If the connection is configured on another WX switch, this field contains a hyphen (-).
Serial Id	Serial ID of the Distributed MAP.
AP IP Address	IP address assigned by DHCP to the Distributed MAP.
WX IP Address	System IP address of the WX switch on which the MAP has an active connection. This is the switch that the MAP used for booting and configuration and is using for data transfer.

See Also

- **display ap config** on page 316
- **display ap global** on page 345
- **display ap unconfigured** on page 347

display ap global

Displays connection information for Distributed MAPs configured on a WX.

Syntax — `display ap global [ap-number | serial-id serial-ID]`

- `ap-number` — Index value that identifies the MAP on the WX.
- `serial-id serial-ID` — MAP access point serial ID.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. Version 6.0 removed the **dap** option.

Usage — Connections are shown only for the Distributed MAPs that are configured on the WX switch from which you enter the command, and only for the Mobility Domain the switch is in.

To show information only for Distributed MAPs that have active connections, use the **display ap connection** command.

Examples — The following command displays configuration information for all the Distributed MAPs configured on a WX switch:

```
WX4400# display ap global
Total number of entries: 8
  AP Serial Id      WX IP Address  Bias
-----
1   M9DE48B012F00  10.3.8.111    HIGH
-   M9DE48B012F00  10.4.3.2      LOW
2   M9DE48B123400  10.3.8.111    LOW
-   M9DE48B123400  10.4.3.2      HIGH
17  M9DE48B123600  10.3.8.111    HIGH
-   M9DE48B123600  10.4.3.2      LOW
18  M9DE48B123700  10.3.8.111    LOW
-   M9DE48B123700  10.4.3.2      HIGH
```

Table 66 describes the fields in this display.

Table 66 Output for display ap global

Field	Description
AP	ID assigned to the Distributed MAP. Note: AP numbers are listed only for Distributed MAPs configured on this WX switch. If the field contains a hyphen (-), the Distributed MAP configuration displayed in the row of output is on another WX switch.
Serial Id	Serial ID of the Distributed MAP.
WX IP Address	System IP address of the WX switch on which the Distributed MAP is configured. A separate row of output is displayed for each WX switch on which the Distributed MAP is configured.
Bias	Bias of the WX switch for the MAP: <ul style="list-style-type: none"> ▪ High ▪ Low

See Also

- **display ap config** on page 316
- **display ap connection** on page 343
- **display ap unconfigured** on page 347
- **set ap** on page 87
- **set ap bias** on page 367

display ap unconfigured

Displays Distributed MAPs that are physically connected to the network but that are not configured on any WX switches.

Syntax — `display ap unconfigured`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. Version 6.0 removed the **dap** option.

Usage — This command also displays a MAP that is directly connected to a WX switch, if the WX port to which the MAP is connected is configured as a network port instead of a MAP access port, and if the network port is a member of a VLAN.

If a Distributed MAP is configured on a WX switch in another Mobility Domain, the MAP can appear in the output until the MAP is able to establish a connection with a WX switch in its Mobility Domain. After the MAP establishes a connection, the entry for the MAP ages out and no longer appears in the command's output.

Entries in the command output's table age out after two minutes.

Examples — The following command displays information for two Distributed MAPs that are not configured:

```
WX1200# display ap unconfigured
Total number of entries: 2
Serial Id      Model  IP Address      Port  Vlan
-----
M9DE48B012F00 AP2750 10.3.8.54       5     default
M9DE48B123400 AP2750 10.3.8.57       6     vlan-eng
```

Table 67 describes the fields in this display.

Table 67 Output for display ap unconfigured

Field	Description
Serial Id	Serial ID of the MAP.
Model	MAP model number.

Table 67 Output for display ap unconfigured (continued)

IP Address	IP address of the MAP. This is the address that the MAP receives from a DHCP server. The MAP uses this address to send a Find WX message to request configuration information from WX switches. However, the MAP cannot use the address to establish a connection unless the MAP first receives a configuration from a WX switch.
Port	Port number on which this WX switch received the MAP Find WX message.
VLAN	VLAN on which this WX switch received the MAP's Find WX message.

See Also

- **display ap connection** on page 343
- **display ap global** on page 345

**display
load-balancing
group**

Displays an RF load balancing group's member radios and current load for each radio.

Syntax — **display load-balancing group** {*group-name* | **all**} [*ap-number* **radio** {**1** | **2**}]

- *group-name* — Name of an RF load-balancing group configured on the WX.
- **all** — Displays information for every load-balancing group that has a radio on this WX as a member.
- *ap-name* — Index value that identifies the MAP on the WX.
- **radio** {**1** | **2**} — Displays status information for a radio on an MAP. This option displays information about radios in the same group as the specified radio.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.0. Version 6.0 removed the **dap** option.

Usage — Use this command to display information about the RF load-balancing groups configured on the WX and the individual MAP radios in the load-balancing groups.

Examples — The following command displays information about the MAP radios that are in the same group as radio 1 on MAP 3:

```
Radios in the same load-balancing group as: ap3/radio1
-----
IP address          AP    Radio Overlap
-----
          10.2.28.200    3     1 100/100
```

The following command displays information about RF load balancing group *blue*:

```
Load-balancing group: blue
IP address          AP    Radio Clients
-----
          10.2.28.200    3     1         0
```

Table 57 describes the fields in displayed by the **display load-balancing group** command.

Table 68 Output for display load-balancing group

Field	Description
IP address	The IP address of the MAP in the load-balancing group.
AP	MAP number
Radio	Radio number
Overlap	The amount of overlapping coverage area the specified MAP radio has with the MAP radio in the list. An overlap of 100/100 indicates that the MAP radios have exactly the same coverage area.
Clients	The current client load on the MAP radio.

See also

- **set load-balancing strictness** on page 399
- **set ap radio load balancing on page 389**
- **set ap local-switching mode** on page 379

display radio-profile

Displays radio profile information.

Syntax — `display radio-profile {name | ?}`

- *name* — Displays information about the named radio profile.
- *?* — Displays a list of radio profiles.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. Name of the backoff timer field changed from Client Backoff Timer to Power Backoff Timer and new fields added in MSS Version 4.0:

- Countermeasures
- Active-Scan
- WMM enabled

Version 4.2 has the following changes:

- WMM enabled field renamed to QoS Mode.
- Long Retry Limit and Short Retry Limit fields moved to **display service-profile** output. (These options are now configurable on a service-profile basis instead of a radio-profile basis.)
- Allow 802.11g clients only field removed. (This option is now configured using the **set service-profile transmit-rates** command.)

Usage — MSS contains a *default* radio profile. 3Com recommends that you do not change this profile but instead keep the profile for reference.

Examples — The following command shows radio profile information for the *default* radio profile:

```
WX4400# display radio-profile default
Beacon Interval:      100      DTIM Interval:      1
Max Tx Lifetime:     2000      Max Rx Lifetime:    2000
RTS Threshold:       2346      Frag Threshold:     2346
Long Preamble:       no        Tune Channel:       yes
Tune Power:          no        Tune Channel Interval: 3600
Tune Power Interval: 600      Channel Holddown:   300
Power Backoff Timer: 10        Countermeasures:    none
Active-Scan:         yes        QoS Mode:           wmm
```

Table 69 describes the fields in this display.

Table 69 Output for display radio-profile

Field	Description
Beacon Interval	Rate (in milliseconds) at which each MAP radio in the profile advertises the beacons SSID.
DTIM Interval	Number of times after every beacon that each MAP radio in the radio profile sends a delivery traffic indication map (DTIM).
Max Tx Lifetime	Number of milliseconds that a frame <i>received</i> by a radio in the radio profile can remain in buffer memory.
Max Rx Lifetime	Number of milliseconds that a frame <i>scheduled to be transmitted</i> by a radio in the radio profile can remain in buffer memory.
RTS Threshold	Minimum length (in bytes) a frame can be for a radio in the radio profile to use the RTS/CTS method to send the frame. The RTS/CTS method clears the air of other traffic to avoid corruption of the frame due to a collision with another frame.
Frag Threshold	Maximum length (in bytes) a frame is allowed to be without being fragmented into multiple frames before transmission by a radio in the radio profile.
Long Preamble	Indicates whether an 802.11b radio that uses this radio profile advertises support for frames with long preambles only: <ul style="list-style-type: none"> ▪ YES — Advertises support for long preambles only. ▪ NO — Advertises support for long and short preambles.
Tune Channel	Indicates whether RF Auto-Tuning is enabled for dynamically setting and tuning channels.
Tune Power	Indicates whether RF Auto-Tuning is enabled for dynamically setting and tuning power levels.
Tune Channel Interval	Interval, in seconds, at which RF Auto-Tuning decides whether to change the channels on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio channels if needed.
Tune Power Interval	Interval, in seconds, at which RF Auto-Tuning decides whether to change the power level on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio power levels if needed.

Table 69 Output for display radio-profile (continued)

Field	Description
Channel Holddown	Minimum number of seconds a radio in a radio profile must remain at its current channel assignment before RF Auto-Tuning can change the channel.
Countermeasures	Indicates whether countermeasures are enabled.
Active-Scan	Indicates whether the active-scan mode of RF detection is enabled.
QoS Mode	<p>Indicates the Quality-of-Service setting for MAP radio forwarding queues:</p> <ul style="list-style-type: none"> ▪ wmm—MAP forwarding queues provide standard priority handling for WMM devices. ▪ svp—MAP forwarding queues are optimized for SpectraLink Voice Priority (SVP). <p>For information about the QoS modes, see the “Configuring Quality of Service” chapter in the <i>Wireless LAN Switch and Controller Configuration Guide</i>.</p>
Service profiles	<p>Service profiles mapped to this radio profile. Each service profile contains an SSID and encryption information for that SSID.</p> <p>Note: When you upgrade from 2.x, MSS creates a default-dot1x service profile for encrypted SSIDs and a default-clear service profile for unencrypted SSIDs. These default service profiles contain the default encryption settings for crypto SSIDs and clear SSIDs, respectively.</p>

See Also

- **set radio-profile active-scan** on page 400
- **set radio-profile auto-tune channel-config** on page 402
- **set radio-profile auto-tune channel-holddown** on page 403
- **set radio-profile auto-tune channel-interval** on page 404
- **set radio-profile auto-tune power-config** on page 406
- **set radio-profile auto-tune power-interval** on page 407
- **set radio-profile beacon-interval** on page 409
- **set radio-profile countermeasures** on page 410
- **set radio-profile dtim-interval** on page 412
- **set radio-profile frag-threshold** on page 413
- **set radio-profile max-rx-lifetime** on page 414

- **set radio-profile max-tx-lifetime** on page 415
- **set radio-profile mode** on page 416
- **set radio-profile preamble-length** on page 419
- **set radio-profile qos-mode** on page 420
- **set radio-profile rts-threshold** on page 423

display service-profile

Displays service profile information.

Syntax — `display service-profile {name | ?}`

- *name* — Displays information about the named service profile.
- *?* — Displays a list of service profiles.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. New fields added to indicate the configured SSID default attributes in the service profile. Version 4.2 added the following fields:

- Proxy ARP
- DHCP restrict
- No broadcast
- Short retry limit (moved from **display radio-profile** output)
- Long retry limit (moved from **display radio-profile** output)
- Sygate On-Demand (SODA)
- Enforce SODA checks:
- SODA remediation ACL
- Custom success web-page
- Custom failure web-page
- Custom logout web-page
- Custom agent-directory
- Static COS
- COS

- CAC mode
- CAC sessions
- User idle timeout
- Idle client probing
- Web Portal Session Timeout
- Transmit rates for 11a / 11b / 11g:
 - beacon rate
 - multicast rate
 - mandatory rate
 - standard rates
 - disabled rates

Version 6.0 removed the **dap** option, and added these new fields:

- Client DSCP
- Mesh enabled
- Bridging enabled
- Load Balance Exempt
- Web Portal Logout
- Custom Web Portal Logout URL

Examples — The following command displays information for service profile *spl*:

```

WX1200# display service-profile spl
ssid-name:                corp2      ssid-type:                crypto
Beacon:                   yes      Proxy ARP:               no
DHCP restrict:            no      No broadcast:            no
Short retry limit:        5      Long retry limit:        5
Auth fallthru:            none    Sygate On-Demand (SODA): no
Enforce SODA checks:      yes     SODA remediation ACL:
Custom success web-page:  Custom failure web-page:
Custom logout web-page:   Custom agent-directory:
Static COS:                no      COS:                     0
CAC mode:                  none    CAC sessions:            14
User idle timeout:         180    Idle client probing:     yes
Web Portal Session Timeout: 5
WEP Key 1 value:           <none>  WEP Key 2 value:         <none>
WEP Key 3 value:           <none>  WEP Key 4 value:         <none>
WEP Unicast Index:        1      WEP Multicast Index:    1
Shared Key Auth:          NO
WPA enabled:
  ciphers: cipher-tkip
  authentication: 802.1X
  TKIP countermeasures time: 60000ms
vlan-name = orange
session-timeout = 300
service-type = 2
11a beacon rate:          6.0      multicast rate:           AUTO
11a mandatory rate: 6.0,12.0,24.0 standard rates: 9.0,18.0,36.0,48.0,54.0
11b beacon rate:          2.0      multicast rate:           AUTO
11b mandatory rate: 1.0,2.0 standard rates: 5.5,11.0
11g beacon rate:          2.0      multicast rate:           AUTO
11g mandatory rate: 1.0,2.0,5.5,11.0 standard rates: 6.0,9.0,12.0,18.0,24.0,
36.0,48.0,54.0

```

Table 70 describes the fields in this display.

Table 70 Output for display service-profile

Field	Description
ssid-name	Service set identifier (SSID) managed by this service profile.
ssid-type	SSID type: <ul style="list-style-type: none"> ▪ crypto — Wireless traffic for the SSID is encrypted. ▪ clear — Wireless traffic for the SSID is unencrypted.
beacon	Indicates whether the radio sends beacons, to advertise the SSID: <ul style="list-style-type: none"> ▪ no ▪ yes
Proxy ARP	Indicates whether proxy ARP is enabled. When this feature is enabled, MSS answers ARP requests on behalf of wireless clients.
DHCP restrict	Indicates whether DHCP Restrict is enabled. When this feature is enabled, MSS allows only DHCP traffic for a new client until the client has successfully completed authentication and authorization.
No broadcast	Indicates whether broadcast restriction is enabled. When this feature is enabled, MSS sends ARP requests and DHCP Offers and Acks as unicasts to their target clients instead of forwarding them as broadcasts.
Short retry limit	Number of times a radio serving the service-profile's SSID can send a short unicast frame without receiving an acknowledgment.
Long retry limit	Number of times a radio serving the service-profile's SSID can send a long unicast frame without receiving an acknowledgment. A long unicast frame is a frame that is <i>equal to or longer than</i> the RTS threshold.
auth-fallthru	Secondary (fallthru) encryption type when a user tries to authenticate but the WX switch managing the radio does not have an authentication rule with a userglob that matches the username. <ul style="list-style-type: none"> ▪ last-resort — Automatically authenticates the user and allows access to the SSID requested by the user, without requiring a username and password. ▪ none—Denies authentication and prohibits the user from accessing the SSID. ▪ web-auth — Redirects the user to a web page for login to the SSID.

Table 70 Output for display service-profile (continued)

Field	Description
Sygate On-Demand (SODA)	Whether SODA functionality is enabled for the service profile. When SODA functionality is enabled, connecting clients download SODA agent files, which perform security checks on the client.
Enforce SODA checks	Whether a client is allowed access to the network after it has downloaded and run the SODA agent security checks. When SODA functionality is enabled, and the WX switch is configured to enforce SODA checks, then a connecting client must download the SODA agent files and pass the checks in order to gain access to the network.
SODA remediation ACL	The name of the ACL to be applied to the client if it fails the SODA agent checks. If no remediation ACL is specified, then a client is disconnected from the network if it fails the SODA agent checks.
Custom success web-page	The name of the user-specified page that the client loads upon successful completion of the SODA agent checks. If no page is specified, then the success page is generated dynamically.
Custom failure web-page	The name of the user-specified page that the client loads if it fails SODA agent checks. If no page is specified, then the failure page is generated dynamically.
Custom logout web-page	The name of the user-specified page that the client loads upon logging out of the network, either by closing the SODA virtual desktop, or by requesting the page. If no page is specified, then the client is disconnected without loading a logout page.
Custom agent-directory	The name of the directory for SODA agent files on the WX switch, if different from the default. By default, SODA agent files are stored in a directory with the same name as the service profile.
Static COS	Indicates whether static CoS assignment is enabled. When this feature is enabled, MAPs assign the CoS value in the COS field to all user traffic forwarded by the MAP.
COS	CoS value assigned by the MAP to all user traffic, if static CoS is enabled. (If static CoS is disabled, WMM or ACLs are used to assign CoS.)
Client DSCP	Whether packets are classified based on client DSCP level instead of 802.11 priority.

Table 70 Output for display service-profile (continued)

Field	Description
CAC mode	Call Admission Control mode: <ul style="list-style-type: none"> ■ none—CAC is disabled. ■ session—CAC is based on the number of active user sessions. If a MAP radio reaches the maximum number of active user sessions specified in the CAC session field, the MAP radio rejects new connection attempts.
CAC sessions	Maximum number of user sessions that can be active on a MAP radio at one time, if the CAC mode is session. (If the CAC mode is none, this value is not used.)
User idle timeout	Indicates how many seconds a user session can remain idle (indicated by no user traffic and no reply to client keepalive probes) before the session is changed to the Disassociated state.
Idle client probing	Indicates whether client keepalive probes are enabled.
Web Portal Session Timeout	When a Web Portal WebAAA session is placed in the Deassociated state, how many seconds the session can remain in that state before being terminated automatically.
Mesh enabled	Whether WLAN mesh services are enabled for the service profile.
Bridging enabled	Whether wireless bridging is enabled for this service profile.
Load Balance Exempt	Whether the MAP radios managed by this service profile are exempted (do not participate in) RF load balancing.
Web Portal Logout	Whether the Web Portal WebAAA logout functionality has been enabled.
Custom Web Portal Logout URL	If configured, the URL that Web Portal WebAAA users can access in order to terminate their sessions.
WEP Key 1 value	State of static WEP key number 1. Radios can use this key to encrypt traffic with static Wired-Equivalent Privacy (WEP): <p>none — The key is not configured.</p> <p>preset — The key is configured.</p> <p>Note: The WEP parameters apply to traffic only on the encrypted SSID.</p>
WEP Key 2 value	State of static WEP key number 2: <ul style="list-style-type: none"> ■ none — The key is not configured. ■ preset — The key is configured.

Table 70 Output for display service-profile (continued)

Field	Description
WEP Key 3 value	State of static WEP key number 3: <ul style="list-style-type: none"> ▪ none — The key is not configured. ▪ preset — The key is configured.
WEP Key 4 value	State of static WEP key number 4: <ul style="list-style-type: none"> ▪ none — The key is not configured. ▪ preset — The key is configured.
WEP Unicast Index	Index of the static WEP key used to encrypt unicast traffic on an encrypted SSID.
WEP Multicast Index	Index of the static WEP key used to encrypt multicast traffic on an encrypted SSID.
Shared Key Auth	Indicates whether shared-key authentication is enabled.
WPA enabled or RSN enable	Indicates that the Wi-Fi Protected Access (WPA) information element (IE) is enabled. Additional fields display the settings of other WPA parameters: <ul style="list-style-type: none"> ▪ ciphers — Lists the WPA cipher suites advertised by radios in the radio profile mapped to this service profile. ▪ authentication — Lists the authentication methods supported for WPA or RSN clients: <ul style="list-style-type: none"> 802.1X — dynamic authentication PSK — preshared key authentication ▪ TKIP countermeasures time — Indicates the amount of time (in ms) MSS enforces countermeasures following a second message integrity code (MIC) failure within a 60-second period. <p>Note: These fields are displayed only when the WPA IE or RSN IE is enabled.</p>
vlan-name, session-timeout, service-type	These are examples of authorization attributes that are applied by default to a user accessing the SSID managed by this service profile (in addition to any attributes assigned to the user by a RADIUS server or the local database). <p>Attributes are listed here only if they have been configured as default attribute settings for the service profile.</p> <p>See Table 44 on page 262 for a list of authorization attributes and values that can be assigned to network users.</p>

Table 70 Output for display service-profile (continued)

Field	Description
11a / 11b / 11g transmit rate fields	<p>Data transmission rate settings for each radio type:</p> <ul style="list-style-type: none"> ■ beacon rate—Data rate of beacon frames sent by MAP radios. ■ multicast rate—Data rate of multicast frames sent by MAP radios. If the rate is auto, the MAP sets the multicast rate to the highest rate that can reach all clients connected to the radio. ■ mandatory rates—Set of data transmission rates that clients are required to support in order to associate with an SSID on a MAP radio. A client must support at least one of the mandatory rates. ■ standard rates—The set of valid rates that are neither mandatory nor disabled. These rates are supported for data transmission from the MAP radios. ■ disabled rates—Data transmission rates that MAP radios will not use to transmit data. (The radios will still accept frames from clients at disabled data rates.)

See Also

- **set service-profile auth-dot1x** on page 433
- **set service-profile auth-fallthru** on page 434
- **set service-profile auth-psk** on page 435
- **set service-profile auth-psk** on page 435
- **set service-profile beacon** on page 436
- **set service-profile cac-mode** on page 438
- **set service-profile cac-session** on page 439
- **set service-profile cipher-ccmp** on page 440
- **set service-profile cipher-tkip** on page 441
- **set service-profile cipher-wep104** on page 442
- **set service-profile cipher-wep40** on page 443
- **set service-profile cos** on page 444
- **set service-profile dhcp-restrict** on page 445
- **set service-profile idle-client-probing** on page 446
- **set service-profile long-retry-count** on page 449

- **set service-profile no-broadcast** on page 451
- **set service-profile proxy-arp** on page 452
- **set service-profile psk-phrase** on page 453
- **set service-profile psk-raw** on page 454
- **set service-profile rsn-ie** on page 455
- **set service-profile shared-key-auth** on page 456
- **set service-profile short-retry-count** on page 456
- **set service-profile soda mode** on page 462
- **set service-profile ssid-name** on page 465
- **set service-profile ssid-type** on page 466
- **set service-profile static-cos** on page 467
- **set service-profile tkip-mc-time** on page 466
- **set service-profile transmit-rates** on page 468
- **set service-profile user-idle-timeout** on page 471
- **set service-profile web-portal-form** on page 473
- **set service-profile web-portal-session-timeout** on page 477
- **set service-profile wep active-multicast- index** on page 478
- **set service-profile wep active-unicast- index** on page 479
- **set service-profile wep key-index** on page 480
- **set service-profile wpa-ie** on page 481

reset ap

Restarts a MAP access point.

Syntax — `reset ap ap-number`

- `ap ap-number` — Index value that identifies the MAP on the WX.
- `dap dap-num` — Number of a Distributed MAP to reset.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. Version 6.0 removed the **dap** option.

Usage — When you enter this command, the MAP drops all sessions and reboots.



CAUTION: *Restarting a MAP can cause data loss for users who are currently associated with the MAP.*

Examples — The following command resets MAP 7:

```
WX1200# reset ap 7
This will reset specified AP devices.
Would you like to continue? (y/n)y
success: rebooting ap attached to port 7
```

set ap auto

Creates a profile for automatic configuration of MAPs.

Syntax — `set ap auto`

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.0. Version 6.0 removed the **dap** option.

Usage — Table 71 lists the configurable profile parameters and their defaults. The only parameter that requires configuration is the profile mode. The profile is disabled by default. To use the profile to configure Distributed MAPs, you must enable the profile using the **set ap auto mode enable** command.

The profile uses the *default* radio profile by default. You can change the profile using the **set ap auto radio radio-profile** command. You can use **set ap auto** commands to change settings for the parameters listed in Table 71. (The commands are listed in the “See Also” section.)

Table 71 Configurable Profile Parameters for Distributed MAPs

Parameter	Default Value
MAP Parameters	
bias	high
blink	disable
(Not shown in display ap config output)	
force-image-download	disable (NO)
group (load balancing group)	none
mode	disabled
persistent	none
upgrade-firmware (boot-download-enabled)	enable (YES)
Radio Parameters	
radio num auto-tune max-power	default
radio num mode	enabled
radio num radio-profile	default
radiotype	11g (or 11b for country codes where 802.11g is not allowed)

Examples — The following command creates a profile for automatic Distributed MAP configuration:

```
WX1200# set ap auto
success: change accepted.
```

See Also

- **set ap auto mode** on page 366
- **set ap auto persistent** on page 364
- **set ap auto radiotype** on page 365
- **set ap bias** on page 367

- **set ap blink** on page 368
- **set ap group** on page 379
- **set ap radio auto-tune max-power** on page 384
- **set ap radio auto-tune max-retransmissions** on page 385
- **set ap radio link-calibration** on page 388
- **set ap radio mode** on page 391
- **set ap radio radio-profile** on page 392
- **set ap upgrade-firmware** on page 396

set ap auto persistent

Converts a temporary MAP configuration created by the MAP configuration profile into a persistent MAP configuration on the WX.

Syntax — `set ap auto persistent [ap-number | all]`

- **ap-number** — Index value that identifies the MAP on the WX.
- **all** — Converts the configurations of all Auto-APs being managed by the switch into permanent configurations.

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.0. Version 6.0 removed the **dap** option.

Usage — To display the Distributed MAP numbers assigned to Auto-MAPs, use the **display ap status auto** command.

Examples — The following command converts the configuration of Auto-AP 10 into a permanent configuration:

```
WX4400# set ap auto persistent 10
success: change accepted.
```

See Also

- **set ap auto** on page 362
- **set ap auto mode** on page 366
- **set ap auto radiotype** on page 365

set ap auto radiotype

Sets the radio type for single-MAP radios that use the MAP configuration profile.

Syntax — `set ap auto [radiotype {11a | 11b| 11g}]`

- **radiotype {11a | 11b| 11g}** — Radio type. (The 11a option applies only to single-radio models. The 802.11a radio in two-radio models is always 802.11a.):
 - 11a — 802.11a
 - 11b — 802.11b
 - 11g — 802.11g

Defaults — The default radio type for models AP2750, MP-241, and MP-341, and for the 802.11b/g radios in other models is 802.11g in regulatory domains that support 802.11g, or 802.11b in regulatory domains that do not support 802.11g.

Access — Enabled.

History — Version 6.0 removed the dap option.

Examples — The following command sets the radio type to 802.11b:

```
WX4400# set dap auto radiotype 11b
success: change accepted.
```

See Also

- **set ap auto** on page 362
- **set ap auto mode** on page 366
- **set ap auto persistent** on page 364

set ap auto mode Enables a WX profile for automatic Distributed MAP configuration.

Syntax — `set ap auto mode {enable | disable}`

- **enable** — Enables the MAP configuration profile.
- **disable** — Disables the MAP configuration profile.

Defaults — The MAP configuration profile is disabled by default.

Access — Enabled.

History — Introduced in MSS 4.0. Version 6.0 removed the **dap** option.

Usage — You must use the **set ap auto** command to create the profile before you can enable it.

Examples — The following command enables the profile for automatic Distributed MAP configuration:

```
WX4400# set ap auto mode enable
success: change accepted.
```

See Also

- **set ap auto** on page 362
- **set ap auto persistent** on page 364
- **set ap auto radiotype** on page 365
- **set ap bias** on page 367
- **set ap blink** on page 368
- **set ap group** on page 379
- **set ap radio auto-tune max-power** on page 384
- **set ap radio auto-tune max- retransmissions** on page 385
- **set ap radio link-calibration** on page 388
- **set ap radio mode** on page 391
- **set ap radio radio-profile** on page 392
- **set ap upgrade-firmware** on page 396

set ap bias

Changes the bias for a MAP. Bias is the priority of one WX over other WX switches for booting and configuring the MAP.

Syntax — `set ap ap-number auto bias {high | low}`

- `ap ap-number` — Index value that identifies the MAP on the WX.
- `ap auto` — Configures bias for the MAP configuration profile. (See **set ap auto** on page 362.)
- `high` — High bias.
- `low` — Low bias.

Defaults — The default bias is high.

Access — Enabled.

History — Introduced in MSS Version 3.0. Option **auto** added for configuration of the MAP configuration profile. Version 6.0 removed the **dap** option.

Usage — High bias is preferred over low bias. Bias applies only to WX switches indirectly attached to the MAP through an intermediate Layer 2 or Layer 3 network. A MAP always attempts to boot on MAP port 1 first, and if an WX is directly attached on MAP port 1, the MAP always boots from it.

If MAP port 1 is indirectly connected to WX switches through the network, the MAP boots from the WX with the high bias for the MAP. If the bias for all connections is the same, the MAP selects the WX that has the greatest capacity to add more active MAPs. For example, if a MAP is dual homed to two WX4400 wireless LAN switches, and one of the switches has 50 active MAPs while the other WX has 60 active MAPs, the new MAP selects the WX that has only 50 active MAPs.

If the boot request on MAP port 1 fails, the MAP attempts to boot over its port 2, using the same process described above.

MAP selection of a WX is *sticky*. After a MAP selects a WX to boot from, the MAP continues to use that WX for its active data link even if another switch configured with high bias for the MAP becomes available.

Examples — The following command changes the bias for a Distributed MAP to low:

```
WX4400# set dap 1 bias low
success: change accepted.
```

See Also

- **display ap config** on page 316

set ap blink

Enables or disables LED blink mode on a MAP to make it easy to identify. When blink mode is enabled on (MAP-xxx models, the health and radio LEDs alternately blink green and amber. By default, blink mode is disabled.

Syntax — `set {ap ap-number auto blink {enable | disable}}`

- **ap** *ap-number* — Index value that identifies the MAP on the WX.
- **enable** — Enables blink mode.
- **disable** — Disables blink mode.

Defaults — LED blink mode is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0. Option **auto** added for configuration of the MAP configuration profile. Version 6.0 removed the **dap** option.

Usage — Changing the LED blink mode does not alter operation of the MAP access point. Only the behavior of the LEDs is affected.

Examples — The following command enables LED blink mode on the MAP access points connected to ports 3 and 4:

```
WX1200# set ap 3-4 blink enable
success: change accepted.
```


set ap boot-configuration ip

Specifies static IP address information for a Distributed MAP.

Syntax — `set ap ap-number boot-configuration ip ip-addr netmask mask-addr gateway gateway-addr [mode {enable | disable}]`

Syntax — `set dap dap-num boot-ip mode {enable | disable}`

- **ap** *ap-number* — Index value that identifies the MAP on the WX.
- **ip** *ip-addr* — The IP address to be assigned to the MAP, in dotted decimal notation (for example, 10.10.10.10).
- **netmask** *mask-addr* — The subnet mask, in dotted decimal notation (for example, 255.255.255.0).
- **gateway** *gateway-addr* — The IP address of the next-hop router, in dotted decimal notation.
- **mode** {enable | disable} — Enables or disables the static IP address for the MAP.

Defaults — By default MAPs use DHCP to obtain an IP address, rather than a using a manually assigned IP address.

Access — Enabled.

History — Introduced in MSS version 4.2. Version 6.0 removed the **dap** option.

Usage — Normally, Distributed MAPs use DHCP to obtain IP address information. In some installations, DHCP may not be available. In this case, you can assign static IP address information to the MAP, including the MAP IP address and netmask, and default gateway.

If the manually assigned IP information is incorrect, the MAP uses DHCP to obtain its IP address.

Examples — The following command configures MAP 1 to use IP address 172.16.0.42 with a 24-bit netmask, and use 172.16.0.20 as its default gateway:

```
WX4400# set ap 1 boot-configuration ip 172.16.0.42 netmask
255.255.255.0 gateway 172.16.0.20
success: change accepted.
```

See Also

- **clear ap boot-configuration** on page 310
- **display ap boot-configuration** on page 342
- **set ap boot-configuration vlan** on page 375

set ap boot-configuration mesh mode

Enables WLAN mesh services on the MAP.

Syntax — `set ap ap-number boot-configuration mesh mode [mode {enable | disable}]`

- `ap ap-number` — Index value that identifies the MAP on the WX.
- `mode {enable | disable}` — Enables or disables WLAN mesh services for the MAP.

Defaults — Disabled.

Access — Enabled.

History — Introduced in MSS version 6.0.

Usage — Use this command to enable WLAN mesh services for an Mesh AP. Prior to deploying the Mesh AP in its final untethered location, you must connect the MAP to an WX and enter this command to configure the MAP for mesh services.

Examples — The following command enables WLAN mesh services for MAP 7:

```
WX4400# set ap 7 boot-configuration mesh mode enable
success: change accepted.
```

See Also

- **display ap mesh-links** on page 329
- **set ap boot-configuration mesh ssid** on page 373
- **set service-profile mesh** on page 450

set ap boot-configuration mesh psk-phrase

Specifies a preshared key (PSK) phrase that a Mesh AP uses for authentication to its Mesh Portal AP.

Syntax — `set ap ap-number boot-configuration mesh psk-phrase passphrase`

- **ap** *ap-number* — Index value that identifies the MAP on the WX.
- *passphrase* — An ASCII string from 8 to 63 characters long. The string can contain blanks if you use quotation marks at the beginning and end of the string.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — Use this command to configure the preshared key that a Mesh AP uses to authenticate to a Mesh Portal AP. You must connect the MAP to an WX switch and enter this command to configure the MAP for mesh services prior to deploying the Mesh AP in its final untethered location.

MSS converts the passphrase into a 256-bit binary number for system use and a raw hexadecimal key to store in the WX configuration. Neither the binary number nor the passphrase itself is ever displayed in the configuration. To use PSK authentication, you must enable it and you also must enable the WPA IE.

Examples — The following command configures MAP 7 to use passphrase "1234567890123<>?+=&% The quick brown fox jumps over the lazy sl" when authenticating with a Mesh Portal AP

```
WX# set ap 7 boot-configuration mesh psk-phrase
"1234567890123<>?+=&%
success: change accepted.
```

See Also

- **display ap mesh-links** on page 329
- **set ap boot-configuration mesh ssid** on page 373
- **set service-profile mesh** on page 450

**set ap
boot-configuration
mesh psk-raw**

Configures a raw hexadecimal preshared key (PSK) to use for authenticating a Mesh AP to a Mesh Portal AP. Radios use the PSK as a pairwise master key (PMK) to derive unique pairwise session keys for individual WPA clients.

Syntax — `set ap ap-number boot-configuration mesh psk-raw hex`

- **ap** *ap-number* — Index value that identifies the MAP on the WX.
- **hex** — A 64-bit ASCII string representing a 32-digit hexadecimal number. Enter the two-character ASCII form of each hexadecimal number.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — Use this command to configure the preshared key that a Mesh AP uses to authenticate to a Mesh Portal AP. You must connect the MAP to an WX switch and enter this command to configure the MAP for mesh services prior to deploying the Mesh AP in its final untethered location.

MSS converts the hexadecimal into a 256-bit binary number for system use. MSS also stores the hexadecimal key in the WX configuration. The binary number is never displayed in the configuration. To use PSK authentication, you must enable it and you also must enable the WPA IE.

Examples — The following command configures MAP 7 to use a raw PSK to authenticate with a Mesh Portal AP:

```
WX# set ap 7 boot-configuration mesh psk-raw
c25d3fe4483e867d1df96eaacdf8b02451fa0836162e758100f5f6b87965
e59d
success: change accepted.
```

See Also

- **display ap mesh-links** on page 329
- **set ap boot-configuration mesh ssid** on page 373
- **set service-profile mesh** on page 450

**set ap
boot-configuration
mesh ssid**

Specifies the name of the SSID a Mesh AP attempts to associate with when it is booted.

Syntax — `set ap ap-number boot-configuration mesh ssid mesh-ssid`

- **ap** *ap-number* — Index value that identifies the MAP on the WX.
- *mesh-ssid* — Name of the mesh SSID (up to 32 characters).

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — You must connect the MAP to a WX switch and enter this command to specify the mesh SSID prior to deploying the Mesh AP in its final untethered location. When the MAP is booted its untethered location, and it determines that it has no Ethernet link to the network, it then associates with the specified *mesh-ssid*.

Note that when the *mesh-ssid* is specified, the regulatory domain of the WX and the power restrictions are copied to the MAP flash memory. This prevents the Mesh AP from operating outside of regulatory limits after it is booted and before it receives its complete configuration from the WX. Consequently, it is important that the regulatory and antenna information specified on the WX actually reflects the locale where the Mesh AP is to be deployed, in order to avoid regulatory violations.

Examples — The following command configures MAP 7 to attempt to associate with the SSID *wlan-mesh* when booted in an untethered location:

```
WX# set ap 7 boot-configuration mesh ssid wlan-mesh
success: change accepted.
```

- **display ap mesh-links** on page 329
- **set ap boot-configuration mesh mode** on page 370
- **set service-profile mesh** on page 450

set ap boot-configuration switch

Specifies the WX a Distributed MAP contacts and attempts to use as its boot device.

Syntax — `set ap ap-number boot-configuration switch [switch-ip ip-addr] [name name dns ip-addr] [mode {enable | disable}]`

- **ap** ap-number — Index value that identifies the MAP on the WX.
- **switch-ip** ip-addr — The IP address of the WX switch the Distributed MAP should boot from.
- **name** name — The fully qualified domain name of the WX the Distributed MAP should boot from. When both a name and a switch-ip are specified, the MAP uses the name.
- **dns** ip-addr — The IP address of the DNS server used to resolve the specified name of the WX switch.
- **mode** {enable | disable} — Enables or disables the MAP using the specified boot device.

Defaults — By default MAPs use the process described in “Default MAP Boot Process”, in the [Wireless LAN Switch and Controller Configuration Guide](#) to boot from a WX, instead of using a manually specified WX.

Examples — Enabled.

History — Introduced in MSS 4.2. Version 6.0 removed the **dap** option.

Usage — When you specify a boot WX for a distributed MAP to boot from, it boots using the process described in “MAP Boot Process Using Static IP Configuration”, in the [Wireless LAN Switch and Controller Configuration Guide](#).

When a static IP address is specified for a Distributed MAP, there is no preconfigured DNS information or DNS name for the WX the Distributed MAP attempts to use as its boot device. If you configure a static IP address for a Distributed MAP, but do not specify a boot device, then the WX must be reachable via subnet broadcast.

Examples — The following command configures Distributed MAP 1 to use the WX with address 172.16.0.21 as its boot device.

```
WX1200# set ap 1 boot- configuration switch switch-ip
172.16.0.21 mode enable
success: change accepted.
```

The following command configures Distributed MAP 1 to use the WX with the name wxr2 as its boot device. The DNS server at 172.16.0.1 is used to resolve the name of the WX switch.

```
WX4400# set ap 1 boot-configuration switch name wxr2 dns
172.16.0.1 mode enable
success: change accepted.
```

See Also

- **clear ap boot-configuration** on page 310
- **display ap boot-configuration** on page 342
- **set ap boot- configuration ip** on page 369
- **set ap boot-configuration vlan** on page 375

set ap boot-configuration vlan

Specifies 802.1Q VLAN tagging information for a Distributed MAP.

Syntax — `set ap ap-number boot-configuration vlan vlan-tag tag-value [mode {enable | disable}]`

Syntax — `set ap ap-number boot-configuration vlan mode {enable | disable}`

- **ap ap-number** — Index value that identifies the MAP on the WX.
- **vlan-tag tag-value** — The VLAN tag value. You can specify a number from 1 – 4095.
- **mode {enable | disable}** — Enables or disables use of the specified VLAN tag on the Distributed MAP.

Defaults — None.

Examples — Enabled.

History — Introduced in MSS 4.2. Version 6.0 removed the **dap** option.

Usage — When this command is configured, all Ethernet frames emitted from the Distributed MAP are formatted with an 802.1Q tag with a specified VLAN number. Frames sent to the Distributed MAP that are not tagged with this value are ignored.

Examples — The following command configures Distributed MAP 1 to use VLAN tag 100:

```
WX4400# set ap 1 boot-configuration vlan vlan-tag 100 mode
enable
success: change accepted.
```

See Also

- **clear ap boot-configuration** on page 310
- **display ap boot-configuration** on page 342
- **set ap boot-configuration ip** on page 369

set ap contact

Specifies information about the contact information for the MAP.

Syntax — `set ap port-list contact string`

Examples — The following command specifies the contact person as *Bob*:

```
WX4400# set ap 7 contact 'Bob'
success: change accepted.
```

See Also

- **set ap location** on page 379
- **display ap config** on page 316

set ap fingerprint

Verifies a MAP fingerprint on a WX. If MAP-WX security is required by a WX, a MAP can establish a management session with the switch only if you have verified the MAP identity by verifying its fingerprint on the switch.

Syntax — `set ap ap-number fingerprint fingerprint`

- `ap ap-num` — Index value that identifies the MAP on the WX.

- *fingerprint* — The 16-digit hexadecimal number of the fingerprint. Use a colon between each digit. Make sure the fingerprint you enter matches the fingerprint used by the MAP.

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.0. Version 6.0 removed the **dap** option.

Usage — MAPs are configured with an encryption key pair at the factory. The fingerprint for the public key is displayed on a label on the back of the MAP, in the following format:

```
RSA
aaaa:aaaa:aaaa:aaaa:
aaaa:aaaa:aaaa:aaaa
```

If a MAP is already installed and operating, you can use the **display ap status** command to display the fingerprint. The **display ap config** command lists a MAP fingerprint only if the fingerprint has been verified in MSS. If the fingerprint has not been verified, the fingerprint information in the command output is blank.

Examples — The following example verifies the fingerprint for Distributed MAP 8:

```
WX4400# set ap 8 fingerprint
b4:f9:2a:52:37:58:f4:d0:10:75:43:2f:45:c9:52:c3
success: change accepted.
```

See Also

- **display ap config** on page 316
- **display ap status** on page 331
- **set ap security** on page 395

set ap force-image-download

Configures a MAP to download a software image from the WX instead of loading the image locally stored on the MAP.

Syntax — `set ap auto force-image-download {enable | disable}`

- **ap auto**—Configures forced image download for the MAP configuration profile.
- **force-image-download enable**—Enables forced image download.
- **force-image-download disable**—Disables forced image download.

Defaults — Forced image download is disabled by default.

Access — Enabled.

History —Version 5.0Command introduced. Version 6.0Option **dap** removed.

Usage — A change to the forced image download option takes place the next time the MAP is restarted.

Even when forced image download is disabled (the default), the MAP still checks with the WX to verify that the MAP has the latest image, and to verify that the WX is running MSS Version 5.0 or later.

The MAP loads a local image only if the WX is running MSS Version 5.0 or later and does not have a different MAP image than the one in the MAP local storage. If the WX is not running MSS Version 5.0 or later, or the WX has a different version of the MAP image than the current version on the MAP, the MAP loads an image from the WX.

Examples — The following command enables forced image download on Distributed MAP 69:

```
WX1200# set ap 69 force-image-download enable
success: change accepted.
```

See Also

- **display ap config** on page 316

set ap group Deprecated in MSS Version 6.0. To configure RF load balancing, see “set load-balancing mode” on page 398.

set ap location Specifies information about the physical location of a MAP.

Syntax — `set ap port-list location string`

Examples — The following command specifies the location of MAP 7 as *the conference room*:

```
WX4400# set ap 7 location 'the conference room'  
success: change accepted.
```

See Also

- **set ap contact** on page 376
- **display ap config** on page 316

**set ap
local-switching
mode**

Enables local switching for a specified MAP.

Syntax — `set ap ap-number local-switching mode {enable | disable}`]

- *ap-number* — Index value that identifies the MAP on the WX.
- **mode {enable | disable}** — Enables or disables local switching for the MAP.

Defaults — Local switching is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — Local switching allows traffic for specified VLANs to be switched by the MAP itself, instead of being tunneled back to a WX. The VLANs for which local switching is performed are specified in a VLAN profile.

Local switching can be enabled on MSPs that are connected to the WX via an intermediate Layer 2 or Layer 3 network. Local switching is not supported for MAPs that are directly connected to an WX.

If local switching is enabled on an MAP, but no VLAN profile is configured, then a default VLAN profile is used. The default VLAN profile includes a single VLAN named *default* that is not tagged.

Examples — The following command enables local switching for MAP 7:

```
WX# set ap 7 local-switching mode enable
success: change accepted.
```

See Also

- **set ap local-switching vlan-profile** on page 380
- **set vlan profile** on page 127

set ap local-switching vlan-profile

Applies a specified VLAN profile to an MAP to use with local switching.

Syntax — `set ap ap-number local-switching vlan-profile profile name`

- *ap-number* — Index value that identifies the MAP on the WX.
- *profile-name* — The name of a VLAN profile configured on the WX.

Defaults — If local switching is enabled on an MAP, but no VLAN profile is configured, then a default VLAN profile is used. The default VLAN profile includes a single VLAN named *default* that is not tagged.

Access — Enabled.

History — Introduced in MSS Version 6.0.

History — A VLAN profile consists of a list of VLANs and tags. When a VLAN profile is applied to an MAP, traffic for the VLANs specified in the VLAN profile is locally switched by the MAP instead of being tunneled back to an WX.

When applying a VLAN profile causes traffic that had been tunneled to an WX to be locally switched by MAPs, or vice-versa, the sessions of clients associated with the MAPs where the VLAN profile is applied are terminated, and the clients must re-associate with the MAPs.

Examples — The following command specifies that MAP 7 use VLAN profile *locals*:

```
WX# set ap 7 local-switching vlan-profile locals
success: change accepted.
```

See Also

- **clear ap local-switching vlan-profile** on page 307
- **set ap local-switching mode** on page 379
- **set vlan profile** on page 127

set ap name

Changes a MAP name.

Syntax — `set ap ap number name name`

- *ap ap-number* — Index value that identifies the MAP on the WX.
- *name* — Alphanumeric string of up to 16 characters, with no spaces.

Defaults — The default name of a directly attached MAP is based on the port number of the MAP access port attached to the MAP. For example, the default name for a MAP on MAP access port 1 is *MAP01*.

Access — Enabled.

History — Introduced in MSS Version 3.0. Default Distributed MAP name changed from *DMPnum* to *DAPnum* in MSS Version 4.1. Version 6.0 removed the **dap** option.

Examples — The following command changes the name of the MAP on port 1 to *techpubs*:

```
WX1200# set ap 1 name techpubs
success: change accepted.
```

See Also

- **display ap config** on page 316

**set ap radio
antenna-location**

Specifies the location (indoors or outdoors) of an external antenna. Use this command to ensure that the proper set of channels is available on the radio. In some cases, the set of valid channels for a radio differs depending on the location of the antenna, indoors or outdoors.

Syntax — `set ap apnum radio number antenna-location {indoors | outdoors}`

- **ap *apnum***—Index value that identifies the MAP on the WX.
- **radio *number***—Specify radio 1 or radio 2.
- **antenna-location**—Specify antenna location.
- **indoors**—Specifies that the external antenna is installed indoors (inside the building).
- **outdoors**—Specifies that the external antenna is installed outdoors.

Defaults — The default antenna location is indoors.

Access — Enabled.

History —Introduced in MSS 5.0.

Examples — The following command sets the antenna location for radio 1 on Distributed MAP 22 to outdoors:

```
WX2200# set ap 22 radio 1 antenna-location outdoors
success: change accepted.
```

See Also

- **set ap radio antennatype** on page 383

set ap radio antennatype

Sets the model number for an external antenna.

Syntax — `set ap ap-number radio {1|2} antennatype`

`{ANT1060 | ANT1120 | ANT1180 |
ANT5060 | ANT5120 | ANT5180 |
ANT-1360-OUT | ANT-5360-OUT | ANT-5120-OUT | internal}`

- `ap ap-number` — Index value that identifies the MAP on the WX.
- `radio 1` — Radio 1 of the MAP.
- `radio 2` — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- `antennatype {ANT1060 | ANT1120 | ANT1180 | internal}` — 802.11b/g external antenna models:
 - `ANT1060` — 60° 802.11b/g antenna
 - `ANT1120` — 120° 802.11b/g antenna
 - `ANT1180` — 180° 802.11b/g antenna
 - `internal` — uses the internal antenna instead
- `antennatype {ANT5060 | ANT5120 | ANT5180 | internal}` — 802.11a external antenna models:
 - `ANT5060` — 60° 802.11a antenna
 - `ANT5120` — 120° 802.11a antenna
 - `ANT5180` — 180° 802.11a antenna
 - `internal` — uses the internal antenna instead
- `antennatype {ANT-1360-OUT | ANT5360-OUT | ANT5060 | ANT5120-OUT | internal}` — 802.11a external antenna models:
 - `ANT1360-OUT` — 360° 802.11b/g antenna
 - `ANT5360-OUT` — 360° 802.11a antenna
 - `ANT5060-OUT` — 60° 802.11a antenna
 - `ANT5120-OUT` — 120° 802.11a antenna
 - `internal` — uses the internal antenna instead

Defaults — All radios use the internal antenna by default, if the MAP model has an internal antenna. The MP-620 802.11b/g radio uses model ANT-1360-OUT by default. The MP-620 802.11a radio uses model ANT-5360-OUT by default. The AP 3150 802.11b/g radio uses model ANT1060 by default.)

Access — Enabled.

History — Introduced in MSS Version 3.0. Model numbers added for 802.11a external antennas, and the default changed to internal (except for the AP3150) in MSS Version 3.2. Model numbers added for MP-620 external antennas.

Examples — The following command configures the 802.11b/g radio on Distributed MAP 1 to use antenna model ANT1060:

```
WX4400# set ap 1 radio 1 antennatype ANT1060
success: change accepted.
```

See Also

- **display ap config** on page 316

set ap radio auto-tune max-power

Sets the maximum power that RF Auto-Tuning can set on a radio.

Syntax — `set {ap ap-number auto} radio {1 | 2} auto-tune max-power power-level`

- `ap ap-number` — Index value that identifies the MAP on the WX.
- `ap auto` — Sets the maximum power for radios configured by the MAP configuration profile. (See **set ap auto** on page 362.)
- `radio 1` — Radio 1 of the MAP.
- `radio 2` — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- `power-level` — Maximum power setting RF Auto-Tuning can assign to the radio, expressed as the number of decibels in relation to 1 milliwatt (dBm). You can specify a value from 1 up to the maximum value allowed for the country of operation.

The *power-level* can be a value from 1 to 20.

Defaults — The default maximum power setting that RF Auto-Tuning can set on a radio is the highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.

Access — Enabled.

History — Introduced in MSS Version 3.0. Option **auto** added for configuration of the MAP configuration profile.

Examples — The following command sets the maximum power that RF Auto-Tuning can set on radio 1 on the MAP access point on port 6 to 12 dBm.

```
WX1200# set ap 7 radio 1 auto-tune max-power 12
success: change accepted.
```

See Also

- **set ap radio auto-tune max- retransmissions** on page 385
- **set radio-profile auto-tune power-config** on page 406
- **set radio-profile auto-tune power-interval** on page 407

set ap radio auto-tune max-retransmissions

Sets the maximum percentage of client retransmissions a radio can experience before RF Auto-Tuning considers changing the channel on the radio. A high percentage of retransmissions is a symptom of interference on the channel.

Syntax — `set {ap ap-number auto} radio {1 | 2} auto-tune max-retransmissions retransmissions`

- **ap *ap-number*** — Index value that identifies the MAP on the WX..
- **ap auto** — Sets the maximum retransmissions for radios configured by the MAP configuration profile. (See **set ap auto** on page 362.)
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- ***retransmissions*** — Percentage of packets that can result in retransmissions without resulting in a channel change. You can specify from 1 to 100.

Defaults — The default is 10 percent.

Access — Enabled.

History — Introduced in MSS Version 3.0. Option **auto** added for configuration of the MAP configuration profile. Version 6.0 removed the **dap** option.

Usage — A retransmission is a packet sent from a client to a MAP radio that the radio receives more than once. This can occur when the client does not receive an 802.11 acknowledgement for a packet sent to the radio.

If the radio receives only a single copy of a packet that is transmitted multiple times by a client, the packet is not counted by the radio as a retransmission. For example, if a packet is corrupted and the radio does not receive it, but the second copy of the packet does reach the radio, the radio does not count the packet as a retransmission since the radio received only one recognizable copy of the packet.

The interval is 1000 packets. If more than the specified percentage of packets within a group of 1000 packets received by the radio are retransmissions, the radio increases power.

When the percentage of retransmissions exceeds the *max-retransmissions* threshold, the radio does not immediately increase power. Instead, if the data rate at which the radio is sending packets to the client is above the minimum data rate allowed, the radio lowers the data rate by one setting. If the retransmissions still exceed the maximum allowed, the radio continues to lower the data rate, one setting at a time, until either the retransmissions fall within the allowed percentile or the minimum allowed data rate is reached.

If the retransmissions still exceed the threshold after the minimum allowed data rate is reached, the radio increases power by 1 dBm. The radio continues increasing the power in 1 dBm increments until the retransmissions fall below the threshold.

After the retransmissions fall below the threshold, the radio reduces power by 1 dBm. As long as retransmissions remain below the threshold, the radio continues reducing power in 1 dBm increments until it returns to its default power level.



A radio also can increase power, in 1 dBm increments, if a client falls below the minimum allowed data rate. After a radio increases power, all clients must be at the minimum data rate or higher and the maximum retransmissions must be within the allowed percentile, before the radio begins reducing power again.

Examples — The following command changes the max-retransmissions value to 20:

```
WX1200# set ap 6 radio 1 auto-tune max-retransmissions 20
success: change accepted.
```

See Also

- **set ap radio auto-tune max-power** on page 384
- **set radio-profile auto-tune power-config** on page 406
- **set radio-profile auto-tune power-interval** on page 407

set ap radio channel

Sets a MAP radio's channel.

Syntax — `set ap port-list radio {1 | 2} channel channel-number`

- `ap ap-number` — Index value that identifies the MAP on the WX.
- `radio 1` — Radio 1 of the MAP.
- `radio 2` — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- `channel channel-number` — Channel number. The valid channel numbers depend on the country of operation.

Defaults — The default channel depends on the radio type:

- The default channel number for 802.11b/g is 6.
- The default channel number for 802.11a is the lowest valid channel number for the country of operation.

Access — Enabled.

History — Introduced in MSS Version 3.0. Version 6.0 removed the **dap** option.

Usage — You can configure the transmit power of a radio on the same command line. Use the **tx-power** option.

This command is not valid if dynamic channel tuning (RF Auto-Tuning) is enabled.

Examples — The following command configures the channel on the 802.11a radio on the MAP access point connected to port 5:

```
WX1200# set ap 5 radio 1 channel 36
success: change accepted.
```

The following command configures the channel and transmit power on the 802.11b/g radio on the MAP access point connected to port 1:

```
WX1200# set ap 1 radio 1 channel 1 tx-power 10
success: change accepted.
```

See Also

- **display ap config** on page 316
- **set ap radio tx-power** on page 393

set ap radio link-calibration

Configures an MAP radio to emit link calibration packets, which can aid in positioning a Mesh AP.

Syntax — `set ap ap-number radio {1 | 2} link-calibration mode {enable | disable}`

- **ap *ap-number*** — Index value that identifies the MAP on the WX.
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- **mode enable** — Enables link calibration packets for the MAP radio.
- **mode disable** — Disables link calibration packets for the MAP radio.

Defaults — Disabled.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — A Mesh Portal MAP can be configured to emit link calibration packets to assist with positioning the Mesh AP. A link calibration packet is an unencrypted 802.11 management packet of type *Action*. When enabled on an MAP, link calibration packets are sent at a rate of 5 per second.

The MP-620 is equipped with a connector to which an external RSSI meter can be attached during installation. When an RSSI meter is attached to an MP-620 and a calibration packet is received, the MP-620 emits a voltage to the RSSI meter proportional to the received signal strength of the packet. This can aid in positioning the MP-620 where it has a strong signal to the Mesh Portal AP.

Only one radio on an MAP can be configured to send link calibration packets. Link calibration packets are intended to be used only during installation of MAPs; they are not intended to be enabled on a continual basis.

Examples — The following command enables link calibration packets for MAP radio 1 on MAP 7:

```
WX# set ap 7 radio 1 link-calibration mode enable
WX#
```

See Also

- **display ap mesh-links** on page 329
- **set ap boot-configuration mesh ssid** on page 373
- **set service-profile mesh** on page 450

set ap radio load balancing

Disables or enables RF load balancing for an MAP radio.

Syntax — `set ap ap-number radio {1 | 2} load balancing {enable | disable}`

- **ap *ap-number*** — Index value that identifies the MAP on the WX.
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- **enable** — Enables link calibration packets for the MAP radio.

- **disable** — Disables link calibration packets for the MAP radio.

Defaults — Disabled.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — By default, RF load balancing is enabled on all MAP radios. Use this command to disable or re-enable RF load balancing for the specified MAP radio.

RF load balancing can also be disabled or re-enabled globally with the **set load-balancing mode** command. If RF load balancing has been enabled or disabled for a specific MAP radio, then the setting for the individual radio takes precedence over the global setting.

Examples — The following command disables RF load balancing for MAP radio 1 on MAP 7:

```
WX# set ap 7 radio 1 load-balancing disable
WX#
```

See Also

- **set load-balancing strictness** on page 399
- **clear ap radio load-balancing group** on page 311
- **set ap local-switching mode** on page 379
- **display load-balancing group** on page 348

set ap radio load balancing group

Assigns an MAP radio to a load balancing group.

Syntax — `set ap ap-number radio {1 | 2} load-balancing group name [rebalance]`

- **ap *ap-number*** — Index value that identifies the MAP on the WX.
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- **group *name*** — Name of an RF load balancing group to which the MAP radio is assigned. A radio can belong to only one group.

- **rebalance** — Configures the MAP radio to disassociate its client sessions and rebalance them whenever a new MAP radio is added to the load balancing group.

Defaults — By default, MAP radios are not part of an RF load balancing group.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — Assigning radios to specific load balancing groups is optional. When you do this, MSS considers them to have exactly overlapping coverage areas, rather than using signal strength calculations to determine their overlapping coverage. MSS attempts to distribute client sessions across radios in the load balancing group evenly. A radio can be assigned to only one group.

Examples The following command assigns MAP radio 1 on MAP 7 to load balancing group *room1*:

```
WX# set ap 7 radio 1 load-balancing group room1
WX#
```

See Also

- **clear ap radio load-balancing group** on page 311
- **display load-balancing group** on page 348
- **set load-balancing strictness** on page 399
- **set ap local-switching mode** on page 379

set ap radio mode

Enables or disables a radio on a MAP access point.

Syntax — `set ap {ap-number | auto} radio {1 | 2} mode {enable | disable}`

- **ap** *ap-number* — Index value that identifies the MAP on the WX.
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- **mode enable** — Enables a radio.

- **mode disable** — Disables a radio.

Defaults — MAP access point radios are disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0. Option **auto** added for configuration of the MAP configuration profile. Version 6.0 removed the **dap** option.

Usage — To enable or disable one or more radios to which a profile is assigned, use the **set ap radio radio-profile** command. To enable or disable all radios that use a specific radio profile, use the **set radio-profile** command.

Examples — The following command enables radio 1 on the MAP 1:

```
WX1200# set ap 1 radio 1 mode enable
success: change accepted.
```

The following command enables radio 2 on on MAP 1:

```
WX1200# set ap 1 radio 2 mode enable
success: change accepted.
```

See Also

- **clear ap radio** on page 308
- **display ap config** on page 316
- **set ap radio radio-profile** on page 392
- **set radio-profile mode** on page 416

set ap radio radio-profile

Assigns a radio profile to a MAP radio and enables or disables the radio.

Syntax — **set ap** {*ap-number* | **auto**} **radio** {**1** | **2**}
radio-profile *name* **mode** {**enable** | **disable**}

- **ap ap-number** — Index value that identifies the MAP on the WX.
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)

- **radio-profile** *name* — Radio profile name of up to 16 alphanumeric characters, with no spaces.
- **mode enable** — Enables radios on the specified ports with the parameter settings in the specified radio profile.
- **mode disable** — Disables radios on the specified ports.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. Option **auto** added for configuration of the MAP configuration profile. Version 6.0 removed the **dap** option.

Usage — When you create a new profile, the radio parameters in the profile are set to their factory default values.

To enable or disable all radios using a specific radio profile, use **set radio-profile**.

Examples — The following command enables radio 1 on MAP 5 assigned to radio profile *rp1*:

```
WX1200# set ap 5radio 1 radio-profile rp1 mode enable
success: change accepted.
```

See Also

- **clear ap radio** on page 308
- **display radio-profile** on page 350
- **set ap radio mode** on page 391
- **set radio-profile mode** on page 416

set ap radio tx-power

Sets the transmit power of a MAP radio.

Syntax — `set ap ap-number radio {1 | 2} tx-power power-level`

- **ap** *ap-number* — Index value that identifies the MAP on the WX.
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)

- **tx-power** *power-level* — Number of decibels in relation to 1 milliwatt (dBm). The valid values depend on the country of operation.

The maximum transmit power you can configure on any 3Com radio is the maximum allowed for the country in which you plan to operate the radio *or* one of the following values if that value is less than the country maximum: on an 802.11a radio, 11 dBm for channel numbers less than or equal to 64, or 10 dBm for channel numbers greater than 64; on an 802.11b/g radio, 16 dBm for all valid channel numbers for 802.11b, or 14 dBm for all valid channel numbers for 802.11g.

Defaults — The default transmit power on all MAP radio types is the highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.

Access — Enabled.

History — Introduced in MSS Version 3.0. Version 6.0 removed the **dap** option.

Usage — You also can configure a radio channel on the same command line. Use the **channel** option.

This command is not valid if dynamic power tuning (RF Auto-Tuning) is enabled.

Examples — The following command configures the transmit power on the 802.11a radio on the MAP access point connected to port 5:

```
WX1200# set ap 5 radio 1 tx-power 10
success: change accepted.
```

The following command configures the channel and transmit power on the 802.11b/g radio on the MAP access point connected to port 1:

```
WX1200# set ap 1 radio 1 channel 1 tx-power 10
success: change accepted.
```

See Also

- **display ap config** on page 316
- **set ap radio channel** on page 387

set ap security

Sets security requirements for management sessions between a WX and its Distributed MAPs.

This feature applies to Distributed MAPs only, not to directly connected MAPs configured on MAP access ports.



The maximum transmission unit (MTU) for encrypted MAP management traffic is 1498 bytes, whereas the MTU for unencrypted management traffic is 1474 bytes. Make sure the devices in the intermediate network between the WX switch and Distributed MAP can support the higher MTU.

Syntax — `set ap security secsetting {require | optional | none}`

- **secsetting** *secsetting* — Name of the security security setting.
- **require** — Requires all Distributed MAPs to have encryption keys that have been verified in the CLI by an administrator. If a MAP does not have an encryption key or the key has not been verified, the WX does not establish a management session with the MAP.
- **optional** — Allows MAPs to be managed by the switch even if they do not have encryption keys or their keys have not been verified by an administrator. Encryption is used for MAPs that support it.
- **none** — Encryption is not used, even for MAPs that support it.

Defaults — The default setting is **optional**.

Access — Enabled.

History — Introduced in MSS 4.0. Version 6.0 removed the **dap** option.

Usage — This parameter applies to all Distributed MAPs managed by the WX. If you change the setting to **required**, the WX requires Distributed MAPs to have encryption keys. The WX also requires their fingerprints to be verified in MSS. When MAP security is required, a MAP can establish a management session with the WX only if its fingerprint has been verified by you in MSS.

A change to MAP security support does not affect management sessions that are already established. To apply the new setting to a MAP, restart the MAP.

Examples — The following command configures a WX to require Distributed MAPs to have encryption keys:

```
WX4400# set ap security require
```

See Also

- **display ap config** on page 316
- **display ap status** on page 331
- **set ap fingerprint** on page 376

set ap upgrade-firmware

Disables or reenables automatic upgrade of a MAP access point boot firmware.

Syntax — `set ap auto upgrade-firmware {enable | disable}`

- **ap auto** — Configures firmware upgrades for the MAP configuration profile (See “set ap auto” on page 362.)
- **enable** — Enables automatic firmware upgrades.
- **disable** — Disables automatic firmware upgrades.

Defaults — Automatic firmware upgrades of MAP access points are enabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0. Option **auto** added for configuration of the MAP configuration profile. Version 6.0 removed the **dap** option.

Usage — When the feature is enabled on an WX port, a MAP access point connected to that port upgrades its boot firmware to the latest version stored on the WX switch.

Examples — The following command disables automatic firmware upgrades on the MAP access point connected to port 6:

```
WX1200# set ap 6 upgrade-firmware disable
```

See Also

- **display ap config** on page 316

set band-preference Configures MSS to steer clients that support both the 802.11a and 802.11b/g radio bands to a specific radio on an MAP for the purpose of RF load balancing.

Syntax — `set band-preference {none | 11bg | 11a}`

- **none** — When a client supports both 802.11a and 802.11b/g radio bands, does not steer the client to a specific MAP radio.
- **enable** — When a client supports both 802.11a and 802.11b/g radio bands, steers the client to the 802.11b/g radio.
- **disable** — When a client supports both 802.11a and 802.11b/g radio bands, steers the client to the 802.11a radio.

Defaults — By default, clients are not steered to specific MAP radios for RF load balancing.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — Use this command to steer clients that support both the 802.11a and 802.11b/g bands, to a specific radio on an MAP for the purpose of load balancing. This global `iband-preference` option controls the degree that an MAP with two radios attempts to conceal one of its radios from a client with the purpose of steering the client to the other radio.

Examples — The following command steers clients that support both the 802.11a and 802.11b/g bands to the 802.11a radio on an MAP:

```
WX# set band-preference 11a
WX#
```

See Also

- [display load-balancing group on page 348](#)
- [set load-balancing mode on page 398](#)
- [set load-balancing strictness on page 399](#)
- [set ap radio load balancing on page 389](#)

set load-balancing mode

Disables or reenables RF load balancing globally on the WXMAP.

Syntax — `set load-balancing mode {enable | disable}`

- **enable** — Enables RF load balancing globally on the WX.
- **disable** — Disables RF load balancing globally on the WX.

Defaults — RF load balancing is enabled by default.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — By default, RF load balancing is enabled on all MAP radios. Use this command to disable or re-enable RF load balancing globally for all MAP radios managed by the WX.

If RF load balancing has been enabled or disabled for a specific MAP radio, then the setting for the individual radio takes precedence over the global setting.

Examples — The following command globally disables RF load balancing for all MAP radios managed by the WX switch:

```
WX# set load-balancing mode disable
WX#
```

See Also

- **display load-balancing group** on page 348
- **set load-balancing strictness** on page 399
- **set band-preference** on page 397
- **set ap radio load balancing on page 389**

set load-balancing strictness

Controls the degree to which MSS balances the client load among MAPs when performing RF load balancing.

Syntax — **set load-balancing strictness**

{**low** | **med** | **high** | **max**}

- **low** — No clients are denied service. New clients can be steered to other MAPs, but only to the extent that service can be provided to all clients.
- **med** — Overloaded radios steer new clients to other MAPs more strictly than the **low** option. Clients attempting to connect to overloaded radios may be delayed several seconds.
- **high** — Overloaded radios steer new clients to other MAPs more strictly than the **med** option. Clients attempting to connect to overloaded radios may be delayed up to a minute.
- **max** — RF load balancing is strictly enforced. That is, overloaded radios do not respond to new clients at all. A client would not be able to connect during times that all of the detectable MAP radios are overloaded.

Defaults — Low.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — When performing RF load balancing, MSS may attempt to steer clients to less-busy radios in a load-balancing group. To do this, MSS makes MAP radios with heavy client loads less visible to new clients, causing them to associate with MAP radios that have a lighter load.

Use this command to specify how strictly MSS attempts to keep the client load balanced across the MAP radios in the load-balancing group. When *low* strictness is specified (the default), MSS makes heavily loaded MAP radios less visible in order to steer clients to less-busy MAP radios, but ensures that even if all the MAP radios in the group are heavily loaded, clients are not denied service.

At the other end of the spectrum, when *max* strictness is specified, if an MAP radio has reached its maximum client load, MSS makes it invisible to new clients, causing them to attempt to connect to other MAP radios. In the event that all the MAP radios in the group have reached their maximum client load, then no new clients would be able to connect to the network.

Examples The following command sets the RF load balancing strictness to the maximum setting:

```
WX# set load-balancing strictness max
Success: strictness set to "MAX"
```

See Also

- **display load-balancing group** on page 348
- **set load-balancing mode on page 398**
- **set band-preference** on page 397
- **set ap radio load balancing on page 389**

set radio-profile 11g-only

Deprecated in MSS Verion 4.2. To configure radio data rates, see **set service-profile transmit-rates** on page 468.

set radio-profile active-scan

Disables or reenables active RF detection scanning on the MAP radios managed by a radio profile. When active scanning is enabled, MAP radios look for rogue devices by sending *probe any* requests (probe requests with a null SSID name), to solicit probe responses from other access points.

Passive scanning is always enabled and cannot be disabled. During passive scanning, radios look for rogues by listening for beacons and probe responses.

Syntax — `set radio-profile name active-scan {enable | disable}`

- *name* — Radio profile name.
- **enable** — Configures radios to actively scan for rogues.

- **disable** — Configures radios to scan only passively for rogues by listening for beacons and probe responses.

Defaults — Active scanning is enabled by default.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — You can enter this command on any WX in the Mobility Domain. The command takes effect only on that WX.

Examples — The following command disables active scan in radio profile *radprof3*:

```
wx4400# set radio-profile radprof3 active-scan disable
success: change accepted.
```

See Also

- **display radio-profile** on page 350

set radio-profile auto-tune 11a-channel-range

When configured, the MAP 802.11a radio selects a channel from a limited range of available channels or all available channels.

Syntax — `set radio-profile name auto-tune 11a-channel-range {lower-bands | all-bands}`

- *name*—The name of the radio profile to configure the 802.11a channel range.
- **lower-bands**—Only the lower channels are available for the 802.11a radio: 36, 40, 44, 48, 52, 56, 60, or 64.
- **all-bands**—All 802.11a channels are available for the 802.11a radio: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, and 161.

Defaults — None

Access — Enabled

History — Version 6.0 Command introduced.

Usage — Improves the 802.11a radio usage on the network.

Examples — The following command enables the 802.11a radio to select any available channel in the 802.11a range:

```
WX1200# set radio-profile test auto-tune 11a-channel-range
all-bands
success: change accepted.
```

set radio-profile auto-tune channel-config

Disables or reenables dynamic channel tuning (RF Auto-Tuning) for the MAP radios in a radio profile.

Syntax — `set radio-profile name auto-tune channel-config {enable | disable} [ignore-client]`

- *name* — Radio profile name.
- **enable** — Configures radios to dynamically select their channels when the radios are started.
- **disable** — Configures radios to use their statically assigned channels, or the default channels if unassigned, when the radios are started.
- **ignore-clients** — Configures radios to change channels regardless of client status. Without this option, a radio changes the channel only if the radio does not have any active clients on that channel.

Defaults — Dynamic channel assignment is enabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0. No-client changed to ignore-clients in MSS Version 6.0.

Usage — If you disable RF Auto-Tuning for channels, MSS does not dynamically set the channels when radios are first enabled and also does not tune the channels during operation.

If RF Auto-Tuning for channels is enabled, MSS does not allow you to manually change channels.

RF Auto-Tuning of channels on 802.11a radios uses only the bottom eight channels in the band (36, 40, 44, 48, 52, 56, 60, and 64). To use a higher channel number, you must disable RF Auto-Tuning of channels on the radio profile the radio is in, and use the **set ap | radio channel** command to statically configure the channel.

Examples — The following command disables dynamic channel tuning for radios in the *rp2* radio profile:

```
WX4400# set radio-profile rp2 auto-tune channel-config
disable
success: change accepted.
```

See Also

- **display radio-profile** on page 350
- **set ap radio channel** on page 387
- **set radio-profile auto-tune channel-holddown** on page 403
- **set radio-profile auto-tune channel-interval** on page 404
- **set radio-profile auto-tune power-config** on page 406

set radio-profile auto-tune channel-holddown

Sets the minimum number of seconds a radio in a radio profile must remain at its current channel assignment before RF Auto-Tuning can change the channel. The channel holddown provides additional stability to the network by preventing the radio from changing channels too rapidly in response to spurious RF anomalies such as short-duration channel interference.

Syntax — `set radio-profile name auto-tune channel-holddown holddown`

- *name* — Radio profile name.
- *holddown* — Minimum number of seconds a radio must remain on its current channel setting before RF Auto-Tuning is allowed to change the channel. You can specify from 0 to 65535 seconds.

Defaults — The default RF Auto-Tuning channel holddown is 900 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The channel holddown applies even if RF anomalies occur that normally cause an immediate channel change.

Examples — The following command changes the channel holddown for radios in radio profile *rp2* to 600 seconds:

```
WX4400# set radio-profile rp2 auto-tune channel-holddown 600
success: change accepted.
```

See Also

- **display radio-profile** on page 350
- **set radio-profile auto-tune channel-config** on page 402
- **set radio-profile auto-tune channel-lockdown** on page 405

set radio-profile auto-tune channel-interval

Sets the interval at which RF Auto-Tuning decides whether to change the channels on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio channels if needed.

Syntax — `set radio-profile name auto-tune channel-interval seconds`

- *name* — Radio profile name.
- *seconds* — Number of seconds RF Auto-Tuning waits before changing radio channels to adjust to RF changes, if needed. You can specify from 0 to 65535 seconds.

Defaults — The default channel interval is 3600 seconds (one hour).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — 3Com recommends that you use an interval of at least 300 seconds (5 minutes).

RF Auto-Tuning can change a radio's channel before the channel interval expires in response to RF anomalies. Even in this case, channel changes cannot occur more frequently than the channel holddown interval.

If you set the interval to 0, RF Auto-Tuning does not reevaluate the channel at regular intervals. However, RF Auto-Tuning can still change the channel in response to RF anomalies.

Examples — The following command sets the channel interval for radios in radio profile *rp2* to 2700 seconds (45 minutes):

```
WX4400# set radio-profile rp2 auto-tune channel-interval 2700
success: change accepted.
```

See Also

- **display radio-profile** on page 350
- **set radio-profile auto-tune channel-config** on page 402
- **set radio-profile auto-tune channel-holddown** on page 403

set radio-profile auto-tune channel-lockdown

Locks down the current channel settings on all radios in a radio profile. The channel settings that are in effect when the command is entered are changed into statically configured channel assignments on the radios. RF Auto-Tuning of channels is then disabled in the radio profile.

Syntax — `set radio-profile name auto-tune channel-lockdown`

- *name* — Radio profile name.

Defaults — By default, when RF Auto-Tuning of channels is enabled, channels continue to be changed dynamically based on network conditions.

Access — Enabled.

History — Introduced in MSS Version 5.0.

Usage — To save this command and the static channel configuration commands created when you enter this command, save the configuration.

Examples — The following command locks down the channel settings for radios in radio profile *rp2*:

```
WX# set radio-profile rp2 auto-tune channel-lockdown
success: change accepted
```

See Also

- **display radio-profile** on page 350
- **set radio-profile auto-tune channel-config** on page 402
- **set radio-profile auto-tune channel-holddown** on page 403
- **set radio-profile auto-tune channel-interval** on page 404
- **set radio-profile auto-tune channel-config** on page 402

set radio-profile auto-tune power-config

Enables or disables dynamic power tuning (RF Auto-Tuning) for the MAP radios in a radio profile.

Syntax — `set radio-profile name auto-tune power-config {enable | disable}`

- *name* — Radio profile name.
- **enable** — Configures radios to dynamically set their power levels when the MAPs are started.
- **disable** — Configures radios to use their statically assigned power levels, or the default power levels if unassigned, when the radios are started.

Defaults — Dynamic power assignment is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — When RF Auto-Tuning for power is disabled, MSS does not dynamically set the power levels when radios are first enabled and also does not tune power during operation with associated clients.

When RF Auto-Tuning for power is enabled, MSS does not allow you to manually change the power level.

Examples — The following command enables dynamic power tuning for radios in the *rp2* radio profile:

```
WX4400# set radio-profile rp2 auto-tune power-config enable
success: change accepted.
```

See Also

- **display radio-profile** on page 350
- **set ap radio auto-tune max-power** on page 384
- **set ap radio auto-tune max- retransmissions** on page 385
- **set radio-profile auto-tune channel-config** on page 402
- **set radio-profile auto-tune power-interval** on page 407

set radio-profile auto-tune power-interval

Sets the interval at which RF Auto-Tuning decides whether to change the power level on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio power levels if needed.

Syntax — `set radio-profile name auto-tune power-interval seconds`

- *name* — Radio profile name.
- *seconds* — Number of seconds MSS waits before changing radio power levels to adjust to RF changes, if needed. You can specify from 1 to 65535 seconds.

Defaults — The default power tuning interval is 600 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command sets the power interval for radios in radio profile *rp2* to 240 seconds:

```
WX4400# set radio-profile rp2 auto-tune power-interval 240
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set ap radio auto-tune max- retransmissions** on page 385
- **set radio-profile auto-tune power-config** on page 406

**set radio-profile
auto-tune
power-lockdown**

Locks down the current power settings on all radios in a radio profile. The power settings that are in effect when the command is entered are changed into statically configured power settings on the radios. RF Auto-Tuning of power is then disabled in the radio profile.

Syntax — **set radio-profile** *name* **auto-tune power-lockdown**

- *name*—Radio profile name.

Defaults — By default, when RF Auto-Tuning of power is enabled, power settings continue change dynamically based on network conditions.

Access — Enabled.

History — Introduced in MSS Version 5.0.

Usage — To save this command and the static power configuration commands created when you enter this command, save the configuration.

Examples — The following command locks down the power settings for radios in radio profile *rp2*:

```
WX1200# set radio-profile rp2 auto-tune power-lockdown
success: change accepted.
```

See Also

- **set ap radio auto-tune max-power** on page 384
- **set radio-profile auto-tune channel-lockdown** on page 405
- **set radio-profile auto-tune power-config** on page 406
- **set radio-profile auto-tune power-interval** on page 407
- **set radio-profile auto-tune power-ramp-interval** on page 409
- **display radio-profile** on page 350

set radio-profile auto-tune power-ramp-interval

Changes the interval at which power is increased or decreased, in 1 dBm increments, on radios in a radio profile until the optimum power level calculated by RF Auto-Tuning is reached.

Syntax — `set radio-profile name auto-tune power-ramp-interval seconds`

- *name*—Radio profile name.
- *seconds*—Number of seconds MSS waits before increasing or decreasing radio power by another 1 dBm. You can specify from 1 to 65535.

Defaults — The default interval is 60 seconds.

Access — Enabled.

History —Introduced in MSS Version 5.0.

Examples — The following command changes the power ramp interval for radios in radio profile *rp2* to 120 seconds:

```
WX1200# set radio-profile rp2 auto-tune power-ramp-interval 120
success: change accepted.
```

See Also

- **set ap radio auto-tune max-power** on page 384
- **set radio-profile auto-tune power-config** on page 406
- **set radio-profile auto-tune power-interval** on page 407
- **set radio-profile auto-tune power-ramp-interval** on page 409
- **display radio-profile** on page 350

set radio-profile beacon-interval

Changes the rate at which each MAP radio in a radio profile advertises its service set identifier (SSID).

Syntax — `set radio-profile name beacon-interval interval`

- *name* — Radio profile name.
- *interval* — Number of milliseconds (ms) between beacons. You can specify from 25 ms to 8191 ms.

Defaults — The beacon interval for MAP radios is 100 ms by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples — The following command changes the beacon interval for radio profile *rp1* to 200 ms:

```
WX4400# set radio-profile rp1 beacon-interval 200
success: change accepted.
```

See Also

- **display radio-profile** on page 350
- **set radio-profile mode** on page 416

set radio-profile countermeasures

Enables or disables countermeasures on the MAP radios managed by a radio profile. Countermeasures are packets sent by a radio to prevent clients from being able to use rogue access points.



CAUTION: *Countermeasures affect wireless service on a radio. When a MAP radio is sending countermeasures, the radio is disabled for use by network traffic, until the radio finishes sending the countermeasures.*

MAP radios can also issue countermeasures against interfering devices. An interfering device is not part of the 3Com network but also is not a rogue. No client connected to the device has been detected communicating with any network entity listed in the forwarding database (FDD) of any WX in the Mobility Domain. Although the interfering device is not connected to your network, the device might be causing RF interference with MAP radios.

Syntax — `set radio-profile name countermeasures {all | rogue | configured | none}`

- *name* — Radio profile name.
- **all** — Configures radios to attack rogues and interfering devices.
- **rogue** — Configures radios to attack rogues only.

- **configured** — Configures radios to attack only devices in the attack list on the WX switch (on-demand countermeasures). When this option is specified, devices found to be rogues by other means, such as policy violations or by determining that the device is providing connectivity to the wired network, are not attacked.
- **none** — Disables countermeasures for this radio profile.

Defaults — Countermeasures are disabled by default.

Access — Enabled.

History — Command introduced in MSS Version 4.0. New option **configured** added to support on-demand countermeasures in MSS Version 4.1.

Examples — The following command enables countermeasures in radio profile *radprof3* for rogues only:

```
WX1200# set radio-profile radprof3 countermeasures rogue
success: change accepted.
```

The following command disables countermeasures in radio profile *radprof3*:

```
WX1200# clear radio-profile radprof3 countermeasures
success: change accepted.
```

The following command causes radios managed by radio profile *radprof3* to issue countermeasures against devices in the WX switch's attack list:

```
WX1200# set radio-profile radprof3 countermeasures configured
success: change accepted.
```

Note that when you issue this command, countermeasures are then issued only against devices in the WX attack list, not against other devices that were classified as rogues by other means.

See Also

- **display radio-profile** on page 350

set radio-profile dtim-interval

Changes the number of times after every beacon that each MAP radio in a radio profile sends a delivery traffic indication map (DTIM). A MAP sends the multicast and broadcast frames stored in its buffers to clients who request them in response to the DTIM.



The DTIM interval applies to both the beacons and the nonbeacons.

Syntax — `set radio-profile name dtim-interval interval`

- *name* — Radio profile name.
- *interval* — Number of times the DTIM is transmitted after every beacon. You can enter a value from 1 through 31.

Defaults — By default, MAP access points send the DTIM once after each beacon.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

The DTIM interval does not apply to unicast frames.

Examples — The following command changes the DTIM interval for radio profile *rp1* to 2:

```
WX4400# set radio-profile rp1 dtim-interval 2
success: change accepted.
```

See Also

- **display radio-profile** on page 350
- **set radio-profile mode** on page 416

set radio-profile frag-threshold

Changes the fragmentation threshold for the MAP radios in a radio profile. The fragmentation threshold is the threshold at which the long-retry-count is applicable instead of the short-retry-count.

The long-retry-count specifies the number of times a radio can send a unicast frame that is equal to or longer than the frag-threshold without receiving an acknowledgment.

The short-retry-count specifies the number of times a radio can send a unicast frame that is shorter than the frag-threshold without receiving an acknowledgment.

Syntax — `set radio-profile name frag-threshold threshold`

- *name* — Radio profile name.
- *threshold* — Maximum frame length, in bytes. You can enter a value from 256 through 2346.

Defaults — The default fragmentation threshold for MAP radios is 2346 bytes.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must disable all radios using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

The frag-threshold does not specify the maximum length a frame is allowed to be without being broken into multiple frames before transmission. The MAPs do not support fragmentation upon transmission, only upon reception.

The frag-threshold does not change the RTS threshold, which specifies the maximum length of a frame before the radio uses the RTS/CTS method to send the frame. To change the RTS threshold, use the **set radio-profile rts-threshold** command instead.

Examples — The following command changes the fragmentation threshold for radio profile *rp1* to 1500 bytes:

```
WX4400# set radio-profile rp1 frag-threshold 1500
success: change accepted.
```

See Also

- **display radio-profile** on page 350
- **set radio-profile mode** on page 416
- **set radio-profile rts-threshold** on page 423
- **set service-profile long-retry-count** on page 449
- **set service-profile short-retry-count** on page 456

**set radio-profile
long-retry**

Deprecated in MSS Version 4.2. In 4.2, this parameter is associated with service profiles instead of radio profiles. See **set service-profile long-retry-count** on page 449.

**set radio-profile
max-rx-lifetime**

Changes the maximum receive threshold for the MAP radios in a radio profile. The maximum receive threshold specifies the number of milliseconds that a frame *received* by a radio can remain in buffer memory.

Syntax — `set radio-profile name max-rx-lifetime time`

- *name* — Radio profile name.
- *time* — Number of milliseconds. You can enter a value from 500 (0.5 second) through 250,000 (250 seconds).

Defaults — The default maximum receive threshold for MAP radios is 2000 ms (2 seconds).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples — The following command changes the maximum receive threshold for radio profile *rp1* to 4000 ms:

```
WX4400# set radio-profile rp1 max-rx-lifetime 4000
success: change accepted.
```

See Also

- **display radio-profile** on page 350
- **set radio-profile mode** on page 416
- **set radio-profile max-tx-lifetime** on page 415

**set radio-profile
max-tx-lifetime**

Changes the maximum transmit threshold for the MAP radios in a radio profile. The maximum transmit threshold specifies the number of milliseconds that a frame *scheduled to be transmitted* by a radio can remain in buffer memory.

Syntax — `set radio-profile name max-tx-lifetime time`

- *name* — Radio profile name.
- *time* — Number of milliseconds. You can enter a value from 500 (0.5 second) through 250,000 (250 seconds).

Defaults — The default maximum transmit threshold for MAP radios is 2000 ms (2 seconds).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples — The following command changes the maximum transmit threshold for radio profile *rp1* to 4000 ms:

```
WX4400# set radio-profile rp1 max-tx-lifetime 4000
success: change accepted.
```

See Also

- **display radio-profile** on page 350
- **set radio-profile mode** on page 416
- **set radio-profile max-rx-lifetime** on page 414

set radio-profile mode

Creates a new radio profile, and disables or reenables all MAP radios that are using a specific profile.

Syntax — `set radio-profile name [mode {enable | disable}]`

- **radio-profile name** — Radio profile name of up to 16 alphanumeric characters, with no spaces.

Use this command without the mode enable or mode disable option to create a new profile.

- **mode enable** — Enables the radios that use this profile.
- **mode disable** — Disables the radios that use this profile.

Defaults — Each radio profile that you create has a set of properties with factory default values that you can change with the other **set radio-profile** commands in this chapter.

Table 72 lists the parameters controlled by a radio profile and their default values.

Table 72 Defaults for Radio Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set to Default Value
active-scan	enable	Sends <i>probe any</i> requests (probe requests with a null SSID name) to solicit probe responses from other access points.
auto-tune	enable	Allows dynamic configuration of channel and power settings by MSS.
beacon-interval	100	Waits 100 ms between beacons.
countermeasures	Not configured	Does not issue countermeasures against any device.
dtim-interval	1	Sends the delivery traffic indication map (DTIM) after every beacon.
frag-threshold	2346	Uses the short-retry-count for frames shorter than 2346 bytes and uses the long-retry-count for frames that are 2346 bytes or longer.
max-rx-lifetime	2000	Allows a received frame to stay in the buffer for up to 2000 ms (2 seconds).

Table 72 Defaults for Radio Profile Parameters (continued)

Parameter	Default Value	Radio Behavior When Parameter Set to Default Value
max-tx-lifetime	2000	Allows a frame that is scheduled for transmission to stay in the buffer for up to 2000 ms (2 seconds).
preamble-length	short	Advertises support for short 802.11b preambles, accepts either short or long 802.11b preambles, and generates unicast frames with the preamble length specified by the client. Note: This parameter applies only to 802.11b/g radios.
qos-mode	wmm	Classifies and marks traffic based on 802.1p and DSCP, and optimizes forwarding prioritization of MAP radios for Wi-Fi Multimedia (WMM).
rts-threshold	2346	Transmits frames longer than 2346 bytes by means of the Request-to-Send/Clear-to-Send (RTS/CTS) method.
service-profile	No service profiles defined	You must configure a service profile. The service profile sets the SSID name and other parameters.

Access — Enabled.

History — Introduced in MSS Version 3.0. Version 4.2 made the following changes:

- Removed the following parameters that no longer apply:
 - 11g-only
 - long-retry
 - short-retry
- **The wmm parameter name changed to qos-mode.**

Usage — Use the command without any optional parameters to create new profile. If the radio profile does not already exist, MSS creates a new radio profile. Use the **enable** or **disable** option to enable or disable all the radios using a profile. To assign the profile to one or more radios, use the **set ap radio radio-profile** command.

To change a parameter in a radio profile, you must first disable all the radios in the profile. After you complete the change, you can reenable the radios.

To enable or disable specific radios without disabling all of them, use the **set ap radio** command.

Examples — The following command configures a new radio profile named *rp1*:

```
WX4400# set radio-profile rp1
success: change accepted.
```

The following command enables the radios that use radio profile *rp1*:

```
WX4400# set radio-profile rp1 mode enable
```

The following commands disable the radios that use radio profile *rp1*, change the beacon interval, then reenable the radios:

```
WX4400# set radio-profile rp1 mode disable
WX4400# set radio-profile rp1 beacon-interval 200
WX4400# set radio-profile rp1 mode enable
```

The following command enables the WPA IE on MAP radios in radio profile *rp2*:

```
WX4400# set radio-profile rp2 wpa-ie enable
success: change accepted.
```

See Also

- **display ap config** on page 316
- **display radio-profile** on page 350
- **set ap radio mode** on page 391
- **set ap radio radio-profile** on page 392

set radio-profile preamble-length

Changes the preamble length for which an 802.11b/g MAP radio advertises support. This command does not apply to 802.11a.

Syntax — `set radio-profile name preamble-length {long | short}`

- *name* — Radio profile name.
- **long** — Advertises support for long preambles.
- **short** — Advertises support for short preambles.

Defaults — The default is **short**.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Changing the preamble length value affects only the support advertised by the radio. Regardless of the preamble length setting (**short** or **long**), an 802.11b/g radio accepts and can generate 802.11b/g frames with either short or long preambles.

If a client associated with an 802.11b/g radio uses long preambles for unicast traffic, the MAP still accepts frames with short preambles but does not transmit frames with short preambles. This change also occurs if the access point overhears a beacon from an 802.11b/g radio on another access point that indicates the radio has clients that require long preambles.

You must disable all radios that use a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples — The following command configures 802.11b/g radios that use the radio profile *rp_long* to advertise support for long preambles instead of short preambles:

```
WX4400# set radio-profile rp_long preamble-length long
success: change accepted.
```

See Also

- **display radio-profile** on page 350
- **set radio-profile mode** on page 416

set radio-profile qos-mode

Sets the prioritization mode for forwarding queues on MAP radios managed by the radio profile.

Syntax — `set radio-profile name qos-mode {svp | wmm}`

- **svp** — Optimizes forwarding prioritization of MAP radios for SpectraLink Voice Priority (SVP).
- **wmm** — Classifies and marks traffic based on 802.1p and DSCP, and optimizes forwarding prioritization of MAP radios for Wi-Fi Multimedia (WMM).

Defaults — The default QoS mode is **wmm**.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — When SVP is enabled, MAP forwarding prioritization is optimized for SpectraLink Voice Priority (SVP) instead of WMM, and the MAP does not tag packets sent to the WX. Otherwise, classification and tagging remain in effect. (For information, see the “Configuring Quality of Service” chapter of the [Wireless LAN Switch and Controller Configuration Guide](#).)

If you plan to use SVP or another non-WMM type of prioritization, you must configure ACLs to tag the packets. (See the “Enabling Prioritization for Legacy Voice over IP” section in the “Configuring and Managing Security ACLs” chapter of the [Wireless LAN Switch and Controller Configuration Guide](#).)

Examples — The following command changes the QoS mode for radio profile *rp1* to SVP:

```
WX4400# set radio-profile rp1 qos-mode svp
success: change accepted.
```

See Also

- **display radio-profile** on page 350
- **set radio-profile mode** on page 416

set radio-profile rfid-mode

Enables MAP radios managed by a radio profile to function as location receivers in an AeroScout Visibility System. An AeroScout Visibility System allows system administrators to track mobile assets using RFID tags.

When you enable RFID mode on a radio profile, radios in the profile can receive and process signals transmitted by RFID tags and relay them with related information to the AeroScout Engine. If the floor plan is modeled in 3WXM, you also can use 3WXM to display the locations of assets.

Syntax — `set radio-profile name rfid-mode {enable | disable}`

- *name*—Radio profile name.
- **enable**—Enables radios to function as asset location receivers.
- **disable**—Disables radios from functioning as asset location receivers.

Defaults — The default is disable.

Access — Enabled.

History —Introduced in MSS Version 5.0.

Examples — The following command enables radios managed by radio profile *rp1* to act as asset location receivers:

```
WX1200# set radio-profile rfid-mode enable
success: change accepted.
```

See Also

- **set radio-profile mode** on page 416
- **display radio-profile** on page 350

set radio-profile rate-enforcement

Configures MSS to enforce data rates, which means that a connecting client must transmit at one of the mandatory or standard rates in order to associate with the MAP.

Syntax — `set radio-profile name rate-enforcement {enable | disable}`

- *name* — Radio profile name.
- **enable** — Enables data rate enforcement for the radios in the radio profile.
- **disable** — Disables data rate enforcement for the radios in the radio profile.

Defaults — Data rate enforcement is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — Each type of radio (802.11a, 802.11b, and 802.11g) providing service to an SSID has a set of radio rates allowed for use when sending beacons, multicast frames, and unicast data. You can configure the rate set for each type of radio, specifying rates in three categories:

Mandatory - Valid 802.11 transmit rates that clients must support in order to associate with the MAP.

Disabled - Valid 802.11 transmit rates are disabled. MAPs do not transmit at the disabled rates.

Standard - Valid 802.11 transmit rates that are not disabled and are not mandatory.

By default, the rate set is not enforced, meaning that a client can associate with and transmit data to the MAP using a disabled data rate, although the MAP does not transmit data back to the client at the disabled rate.

You can use this command to enforce the data rates, which means that a connecting client *must* transmit at one of the mandatory or standard rates in order to associate with the MAP. When data rate enforcement is enabled, clients transmitting at the disabled rates are not allowed to associate with the MAP.

This command is useful if you want to completely prevent clients from transmitting at disabled data rates. For example, you can disable slower data rates so that clients transmitting at these rates do not consume bandwidth on the channel at the expense of clients transmitting at faster rates.

Examples — The following command enables data rate enforcement for radio profile *rp1*:

```
WX# set radio-profile rp1 rate-enforcement mode enable
success: change accepted.
```

See Also

- **display ap counters** on page 319
- **set service-profile transmit-rates** on page 468

set radio-profile rts-threshold

Changes the RTS threshold for the MAP radios in a radio profile. The RTS threshold specifies the maximum length a frame can be before the radio uses the RTS/CTS method to send the frame. The RTS/CTS method clears the air of other traffic to avoid corruption of the frame due to a collision with another frame.

Syntax — `set radio-profile name rts-threshold threshold`

- *name* — Radio profile name.
- *threshold* — Maximum frame length, in bytes. You can enter a value from 256 through 3000.

Defaults — The default RTS threshold for a MAP radio is 2346 bytes.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples — The following command changes the RTS threshold for radio profile *rp1* to 1500 bytes:

```
WX4400# set radio-profile rp1 rts-threshold 1500
success: change accepted.
```

See Also

- **display radio-profile** on page 350
- **set radio-profile mode** on page 416

set radio-profile service-profile

Maps a service profile to a radio profile. All radios that use the radio profile also use the parameter settings, including SSID and encryption settings, in the service profile.

Syntax — `set radio-profile name service-profile name`

- **radio-profile *name*** — Radio profile name of up to 16 alphanumeric characters, with no spaces.
- **service-profile *name*** — Service profile name of up to 16 alphanumeric characters, with no spaces.

Defaults — A radio profile does not have a service profile associated with it by default. In this case, the radios in the radio profile use the default settings for parameters controlled by the service profile. Table 73 lists the parameters controlled by a service profile and their default values.

Table 73 Defaults for Service Profile Parameters

Parameter	Default Value	Radio Behavior When Parameter Set to Default Value
attr	No attributes configured	Does not assign the SSID's authorization attribute values to SSID users, even if attributes are not otherwise assigned.
auth-dot1x	enable	When the Wi-Fi Protected Access (WPA) information element (IE) is enabled, uses 802.1X to authenticate WPA clients.
auth-fallthru	web-auth	Uses WebAAA for users who do not match an 802.1X or MAC authentication rule for the SSID requested by the user.
auth-psk	disable	Does not support using a preshared key (PSK) to authenticate WPA clients.
beacon	enable	Sends beacons to advertise the SSID managed by the service profile.
cac-mode	none	Does not limit the number of active user sessions based on Call Admission Control (CAC).
cac-session	14	If session-based CAC is enabled (cac-mode is set to session), limits the number of active user sessions on a radio to 14.

Table 73 Defaults for Service Profile Parameters (continued)

Parameter	Default Value	Radio Behavior When Parameter Set to Default Value
cipher-ccmp	disable	Does not use Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) to encrypt traffic sent to WPA clients.
cipher-tkip	enable	When the WPA IE is enabled, uses Temporal Key Integrity Protocol (TKIP) to encrypt traffic sent to WPA clients.
cipher-wep104	disable	Does not use Wired Equivalent Privacy (WEP) with 104-bit keys to encrypt traffic sent to WPA clients.
cipher-wep40	disable	Does not use WEP with 40-bit keys to encrypt traffic sent to WPA clients.
cos	0	If static CoS is enabled (static-cos is set to enable), assigns CoS 0 to all data traffic to or from clients.
dhcp-restrict	disable	Does not restrict a client's traffic to only DHCP traffic while the client is being authenticated and authorized.
idle-client-probing	enable	Sends a keepalive packet (a null-data frame) to each client every 10 seconds.
long-retry-count	5	Sends a long unicast frame up to five times without acknowledgment.
no-broadcast	disable	Does not reduce wireless broadcast traffic by sending unicasts to clients for ARP requests, DHCP Offers, and Acks instead of forwarding them as multicasts.
proxy-arp	disable	Does not reply on behalf of wireless clients to ARP requests for client IP addresses. Instead, the radio forwards the ARP Requests as wireless broadcasts.
psk-phrase	No passphrase defined	Uses dynamically generated keys rather than statically configured keys to authenticate WPA clients.
psk-raw	No preshared key defined	Uses dynamically generated keys rather than statically configured keys to authenticate WPA clients.
rsn-ie	disable	Does not use the RSN IE in transmitted frames.

Table 73 Defaults for Service Profile Parameters (continued)

Parameter	Default Value	Radio Behavior When Parameter Set to Default Value
shared-key-auth	disable	Does not use shared-key authentication. This parameter does not enable PSK authentication for WPA. To enable PSK encryption for WPA, use the set radio-profile auth-psk command.
short-retry-count	5	Sends a short unicast frame up to five times without acknowledgment.
soda	disable	Sygate On Demand Agent (SODA) files are not downloaded to connecting clients.
ssid-name	private	Uses the SSID name private .
ssid-type	crypto	Encrypts wireless traffic for the SSID.
static-cos	disable	Assigns CoS based on the QoS mode (wmm or svp) or based on ACLs.
tkip-mc-time	60000	Uses Michael countermeasures for 60,000 ms (60 seconds) following detection of a second MIC failure within 60 seconds.

Table 73 Defaults for Service Profile Parameters (continued)

Parameter	Default Value	Radio Behavior When Parameter Set to Default Value
transmit-rates	802.11a: mandatory: 6.0,12.0,24.0 beacon-rate: 6.0 multicast-rate: auto disabled: none 802.11b: mandatory: 1.0,2.0 beacon-rate: 2.0 multicast-rate: auto disabled: none 802.11g: mandatory: 1.0,2.0,5.5,11.0 beacon-rate: 2.0 multicast-rate: auto disabled: none	Accepts associations only from clients that support one of the mandatory rates. Sends beacons at the specified rate (6 Mbps for 802.11a, 2 Mbps for 802.11b/g). Sends multicast data at the highest rate that can reach all clients connected to the radio. Accepts frames from clients at all valid data rates. (No rates are disabled by default.)
user-idle-timeout	180	Allows a client to remain idle for 180 seconds (3 minutes) before MSS changes the client's session to the Disassociated state.
web-aaa-form	Not configured	For WebAAA users, serves the default login web page or, if configured, the SSID-specific login web page.
web-portal-session-timeout	5	Allows a Web Portal WebAAA session to remain in the Deassociated state 5 seconds before being terminated automatically.

Table 73 Defaults for Service Profile Parameters (continued)

Parameter	Default Value	Radio Behavior When Parameter Set to Default Value
wep key-index	No keys defined	Uses dynamic WEP rather than static WEP. If you configure a WEP key for static WEP, MSS continues to also support dynamic WEP.
wep active-multicast-index	1	Uses WEP key 1 for static WEP encryption of multicast traffic if WEP encryption is enabled and keys are defined.
wep active-unicast-index	1	Uses WEP key 1 for static WEP encryption of unicast traffic if WEP encryption is enabled and keys are defined.
wpa-ie	disable	Does not use the WPA IE in transmitted frames.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — You must configure the service profile before you can map it to a radio profile. You can map the same service profile to more than one radio profile.

You must disable all radios that use a radio profile before you can change parameters in the profile. Use the **set radio-profile mode** command.

Examples — The following command maps service-profile *wpa_clients* to radio profile *rp2*:

```
WX4400# set radio-profile rp2 service-profile wpa_clients
success: change accepted.
```

See Also

- **display radio-profile** on page 350
- **display service-profile** on page 353
- **set service-profile attr** on page 431
- **set service-profile auth-dot1x** on page 433
- **set service-profile auth-fallthru** on page 434
- **set service-profile auth-psk** on page 435
- **set service-profile beacon** on page 436

- **set service-profile cac-mode** on page 438
- **set service-profile cac-session** on page 439
- **set service-profile cipher-ccmp** on page 440
- **set service-profile cipher-tkip** on page 441
- **set service-profile cipher-wep104** on page 442
- **set service-profile cipher-wep40** on page 443
- **set service-profile cos** on page 444
- **set service-profile dhcp-restrict** on page 445
- **set service-profile idle-client-probing** on page 446
- **set service-profile long-retry-count** on page 449
- **set service-profile no-broadcast** on page 451
- **set service-profile proxy-arp** on page 452
- **set service-profile psk-phrase** on page 453
- **set service-profile psk-raw** on page 454
- **set service-profile rsn-ie** on page 455
- **set service-profile shared-key-auth** on page 456
- **set service-profile short-retry-count** on page 456
- **set service-profile soda mode** on page 462
- **set service-profile ssid-name** on page 465
- **set service-profile ssid-type** on page 466
- **set service-profile static-cos** on page 467
- **set service-profile tkip-mc-time** on page 466
- **set service-profile transmit-rates** on page 468
- **set service-profile user-idle-timeout** on page 471
- **set service-profile web-portal-form** on page 473
- **set service-profile web-portal-session-timeout** on page 477
- **set service-profile wep active-multicast- index** on page 478
- **set service-profile wep active-unicast- index** on page 479
- **set service-profile wep key-index** on page 480
- **set service-profile wpa-ie** on page 481

**set radio-profile
short-retry**

Deprecated in MSS Version 4.2. In 4.2, this parameter is associated with service profiles instead of radio profiles. See **set service-profile short-retry-count** on page 456.

**set radio-profile
wmm**

Deprecated in MSS Version 4.2. To enable or disable WMM, see **set radio-profile qos-mode** on page 420.

**set radio-profile
wmm-powersave**

Enables Unscheduled Automatic Powersave Delivery (U-APSD) on MAP radios managed by the radio profile. U-APSD enables WMM clients that use powersave mode to more efficiently request buffered unicast packets from MAP radios.

When U-APSD is enabled, a client can retrieve buffered unicast packets for a traffic priority enabled for U-APSD by sending a QoS data or QoS-Null frame for that priority. U-APSD can be enabled for individual traffic priorities, for individual clients, based on the client's request. A client enables U-APSD for a traffic priority by indicating this preference when (re)associating with the MAP radio.

A client can but is not required to request U-APSD for all four traffic priorities. The MAP radio still buffers packets for all traffic priorities even if the client does not request U-APSD for them. However, to retrieve buffered packets for priorities that are not using U-APSD, a client must send a separate PSpoll for each buffered packet.

Syntax — `set radio-profile name wmm-powersave {enable | disable}`

- *name* — Radio profile name.
- **enable** — Enable U-APSD.
- **disable** — Disables U-APSD.

Defaults — U-APSD is disabled by default..

Access — Enabled.

History — Introduced in MSS 5.0.

Usage — U-APSD is supported only for QoS mode WMM. If WMM is not enabled on the radio profile, use the `set radio-profile qos-mode` command to enable it.

Examples — The following command enables U-APSD on radio profile `rp1`:

```
WX2200# set radio-profile rp1 wmm-powersave enable
success: change accepted.
```

See Also

- **set radio-profile mode** on page 416
- **set radio-profile qos-mode** on page 420
- **display radio-profile** on page 350

set service-profile attr

Configures authorization attributes that are applied by default to users accessing the SSID managed by the service profile. These SSID default attributes are applied in addition to any supplied by the RADIUS server or from the local database.

Syntax — `set service-profile name attr attribute-name value`

- *name* — Service profile name.
- *attribute-name value* — Name and value of an attribute you are using to authorize SSID users for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to network users, see Table 44 on page 262. All of the attributes listed in Table 44 can be used with this command except `ssid`.

Defaults — By default, a service profile does not have any authorization attributes set.

Access — Enabled.

History — Introduced in MSS 4.1.

Usage — To change the value of a default attribute for a service profile, use the `set service-profile attr` command and specify a new value.

The SSID default attributes are applied *in addition* to any attributes supplied for the user by the RADIUS server or the local database. When the same attribute is specified both as an SSID default attribute and through AAA, then the attribute supplied by the RADIUS server or the local database takes precedence over the SSID default attribute. If a location policy is configured, the location policy rules also take precedence over SSID default attributes. The SSID default attributes serve as a fallback when neither the AAA process, nor a location policy, provides them.

For example, a service profile might be configured with the **service-type** attribute set to 2. If a user accessing the SSID is authenticated by a RADIUS server, and the RADIUS server returns the **vlan-name** attribute set to *orange*, then that user will have a total of two attributes set: **service-type** and **vlan-name**.

If the service profile is configured with the **vlan-name** attribute set to *blue*, and the RADIUS server returns the **vlan-name** attribute set to *orange*, then the attribute from the RADIUS server takes precedence; the user is placed in the orange VLAN.

You can display the attributes for each connected user and whether they are set through AAA or through SSID defaults by entering the **display sessions network verbose** command. You can display the configured SSID defaults by entering the **display service-profile** command.

Examples — The following command assigns users accessing the SSID managed by service profile *sp2* to VLAN *blue*:

```
WX4400# set service-prof sp2 attr vlan-name blue
success: change accepted.
```

The following command assigns users accessing the SSID managed by service profile *sp2* to the Mobility Profile *tulip*.

```
WX4400# set service-prof sp2 attr mobility-profile tulip
success: change accepted.
```

The following command limits the days and times when users accessing the SSID managed by service profile *sp2* can access the network, to 5 p.m. to 2 a.m. every weekday, and all day Saturday and Sunday:

```
WX1200# set service-prof sp2 attr time-of-day
Wk1700-0200,Sa,Su
success: change accepted.
```


See Also

- **display service-profile** on page 353
- **display sessions network** on page 620

set service-profile auth-dot1x

Disables or reenables 802.1X authentication of Wi-Fi Protected Access (WPA) clients by MAP radios, when the WPA information element (IE) is enabled in the service profile that is mapped to the radio profile that the radios are using.

Syntax — set service-profile

```
name auth-dot1x {enable | disable}
```

- *name* — Service profile name.
- **enable** — Enables 802.1X authentication of WPA clients.
- **disable** — Disables 802.1X authentication of WPA clients.

Defaults — When the WPA IE is enabled, 802.1X authentication of WPA clients is enabled by default. If the WPA IE is disabled, the **auth-dot1x** setting has no effect.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command does not disable dynamic WEP for non-WPA clients. To disable dynamic WEP for non-WPA clients, enable the WPA IE (if not already enabled) and disable the 40-bit WEP and 104-bit WEP cipher suites in the WPA IE, if they are not already disabled.

To use 802.1X authentication for WPA clients, you also must enable the WPA IE.

If you disable 802.1X authentication of WPA clients, the only method available for authenticating the clients is preshared key (PSK) authentication. To use this, you must enable PSK support and configure a passphrase or key.

Examples — The following command disables 802.1X authentication for WPA clients that use service profile *wpa_clients*:

```
WX4400# set service-profile wpa_clients auth-dot1x disable  
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile auth-psk** on page 435
- **set service-profile psk-phrase** on page 453
- **set service-profile wpa-ie** on page 481

**set service-profile
auth-fallthru**

Specifies the authentication type for users who do not match an 802.1X or MAC authentication rule for an SSID managed by the service profile. When a user tries to associate with an SSID, MSS checks the authentication rules for that SSID for a userglob that matches the username. If the SSID does not have an authentication rule that matches the username, authentication for the user *falls through* to the fallthru method.

The fallthru method is a service profile parameter, and applies to all radios within the radio profiles that are mapped to the service profile.

Syntax — `set service-profile name auth-fallthru
{last-resort | none | web-portal}`

- **last-resort** — Automatically authenticates the user and allows access to the SSID requested by the user, without requiring a username and password.
- **none** — Denies authentication and prohibits the user from accessing the SSID.

The fallthru authentication type **none** is different from the authentication method **none** you can specify for administrative access. The fallthru authentication type **none** denies access to a network user. In contrast, the authentication method **none** allows access to the WX switch by an administrator. (See “set authentication admin” on page 239 and “set authentication console” on page 241.)

- **web-portal** — Serves the user a web page from the WX switch’s nonvolatile storage for secure login to the network.

Defaults — The default fallthru authentication type is **web-auth**.

If a username does not match a userglob in an authentication rule for the SSID requested by the user, the WX switch that is managing the radio the user is connected to redirects the user to a web page located on the WX switch. The user must type a valid username and password on the web page to access the SSID.

Access — Enabled.

History — Introduced in MSS Version 3.0. Option for WebAAA fallthru authentication type changed from **web-auth** to **web-portal** in MSS Version 4.1.

Usage — The **last-resort** fallthru authentication type allows any user to access any SSID managed by the service profile. This method does not require the user to provide a username or password. Use the **last-resort** method only if none of the SSIDs managed by the service profile require secure access.

The **web-auth** authentication type requires additional configuration items. (See the “Configuring AAA for Network Users” chapter of the [Wireless LAN Switch and Controller Configuration Guide](#).)

Examples — The following command sets the fallthru authentication for SSIDs managed by the service profile *rnd_lab* to none:

```
WX4400# set service-profile rnd_lab auth-fallthru none
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set web-portal** on page 278
- **set service-profile web-portal-form** on page 473

set service-profile auth-psk

Enables pre-shared key (PSK) authentication of Wi-Fi Protected Access (WPA) clients by MAP radios in a radio profile, when the WPA information element (IE) is enabled in the service profile.

Syntax — `set service-profile name auth-psk {enable | disable}`

- *name* — Service profile name.
- **enable** — Enables PSK authentication of WPA clients.
- **disable** — Disables PSK authentication of WPA clients.

Defaults — When the WPA IE is enabled, PSK authentication of WPA clients is enabled by default. If the WPA IE is disabled, the **auth-psk** setting has no effect.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command affects authentication of WPA clients only.

To use PSK authentication, you also must configure a passphrase or key. In addition, you must enable the WPA IE.

The WebAAA fallthru authentication type is not supported in conjunction with WPA encryption using preshared keys (PSK) for the same SSID. These options are configurable together but are not compatible. WebAAA traffic is not encrypted, whereas the PSK four-way handshake requires a client to already be authenticated and for encryption to be in place.

Examples — The following command enables PSK authentication for service profile *wpa_clients*:

```
WX4400# set service-profile wpa_clients auth-psk enable
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile auth-dot1x** on page 433
- **set service-profile psk-raw** on page 454
- **set service-profile wpa-ie** on page 481

set service-profile beacon

Disables or reenables beaconing of the SSID managed by the service profile.

A MAP radio responds to an 802.11 *probe any* request with only the beacons SSID(s). For a nonbeaconed SSID, radios respond only to directed 802.11 probe requests that match the nonbeaconed SSID's SSID string.

When you disable beaconing for an SSID, the radio still sends beacon frames, but the SSID name in the frames is blank.

Syntax — `set service-profile name beacon {enable | disable}`

- *name* — Service profile name.

- **enable** — Enables beaconing of the SSID managed by the service profile.
- **disable** — Disables beaconing of the SSID managed by the service profile.

Defaults — Beaconing is enabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command disables beaconing of the SSID managed by service profile *sp2*:

```
WX4400# set service-profile sp2 beacon disable
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set radio-profile beacon-interval** on page 409
- **set service-profile ssid-name** on page 465
- **set service-profile ssid-type** on page 466

set service-profile bridging

Enables wireless bridging for a service profile configured for WLAN mesh services.

Syntax — `set service-profile mesh-service-profile bridging {enable | disable}`

- *mesh-service-profile* — Mesh service profile name.
- **enable** — Enables wireless bridging for the service profile.
- **disable** — Disables wireless bridging for the service profile.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — WLAN mesh services can be used in a wireless bridge configuration, implementing MAPs as bridge endpoints in a transparent Layer 2 bridge. A typical application of wireless bridging is to provide network connectivity between two buildings using a wireless link.

A Mesh Portal AP serving as a bridge endpoint can support up to five Mesh APs serving as bridge endpoints. A Mesh AP serving as a bridge endpoint picks up packets from its wired port and transfers them to the other bridge endpoint. A simple source/destination learning mechanism is used in order to avoid forwarding packets across the bridge unnecessarily.

When wireless bridging is enabled for a service profile, the MAPs with the applied service profile serve as bridge peers. When a Mesh AP associates with a Mesh Portal AP through this service profile, the Mesh Portal AP automatically configures the Mesh AP to operate in bridge mode.

Examples — The following command enables wireless bridging on service profile *sp1*:

```
WX# set service-profile sp1 bridging enable
success: change accepted.
```

See Also

- **display ap mesh-links on page 329**
- **set ap boot-configuration mesh ssid on page 373**
- **set service-profile mesh on page 450**

set service-profile cac-mode

Configures the Call Admission Control (CAC) mode.

Syntax — `set service-profile name cac-mode {none | session}`

- **name** — Service profile name.
- **none** — CAC is not used.
- **session** — CAC is based on the number of active sessions.

Defaults — The default CAC mode is **none**.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Examples — The following command enables session-based CAC on service profile *sp1*:

```
WX4400# set service-profile sp1 cac-mode session
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile cac-session** on page 439

set service-profile cac-session

Specifies the maximum number of active sessions a radio can have when session-based CAC is enabled. When a MAP radio has reached the maximum allowed number of active sessions, the radio refuses connections from additional clients.

Syntax — `set service-profile name cac-session max-sessions`

- **name** — Service profile name.
- **max-sessions** — Maximum number of active sessions allowed on the radio.

Defaults — The default number of sessions allowed is 14.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — This command applies only when the CAC mode is **session**. If the CAC mode is **none**, you can still change the maximum number of sessions, but the setting does not take effect until you change the CAC mode to **session**. To change the CAC mode, use the **set service-profile cac-mode** command.

Examples — The following command changes the maximum number of sessions for radios used by service profile *sp1* to 10:

```
WX4400# set service-profile sp1 cac-session 10
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile cac-mode** on page 438

**set service-profile
cipher-ccmp**

Enables Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption with WPA clients, for a service profile.

Syntax — `set service-profile name cipher-ccmp {enable | disable}`

- *name* — Service profile name.
- **enable** — Enables CCMP encryption for WPA clients.
- **disable** — Disables CCMP encryption for WPA clients.

Defaults — CCMP encryption is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To use CCMP, you must also enable the WPA IE.

Examples — The following command configures service profile *sp2* to use CCMP encryption:

```
WX4400# set service-profile sp2 cipher-ccmp enable
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile cipher-tkip** on page 441
- **set service-profile cipher-wep104** on page 442
- **set service-profile cipher-wep40** on page 443
- **set service-profile wpa-ie** on page 481

set service-profile cipher-tkip

Disables or reenables Temporal Key Integrity Protocol (TKIP) encryption in a service profile.

Syntax — `set service-profile`

`name cipher-tkip {enable | disable}`

- `name` — Service profile name.
- `enable` — Enables TKIP encryption for WPA clients.
- `disable` — Disables TKIP encryption for WPA clients.

Defaults — When the WPA IE is enabled, TKIP encryption is enabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To use TKIP, you must also enable the WPA IE.

Examples — The following command disables TKIP encryption in service profile `sp2`:

```
WX4400# set service-profile sp2 cipher-tkip disable
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile cipher-ccmp** on page 440
- **set service-profile cipher-wep104** on page 442
- **set service-profile cipher-wep40** on page 443
- **set service-profile tkip-mc-time** on page 466
- **set service-profile wpa-ie** on page 481

**set service-profile
cipher-wep104**

Enables dynamic Wired Equivalent Privacy (WEP) with 104-bit keys, in a service profile.

Syntax — `set service-profile name cipher-wep104 {enable | disable}`

- *name* — Service profile name.
- **enable** — Enables 104-bit WEP encryption for WPA clients.
- **disable** — Disables 104-bit WEP encryption for WPA clients.

Defaults — 104-bit WEP encryption is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To use 104-bit WEP with WPA clients, you must also enable the WPA IE.

When 104-bit WEP in WPA is enabled in the service profile, radios managed by a radio profile that is mapped to the service profile can also support non-WPA clients that use dynamic WEP.

To support WPA clients that use 40-bit dynamic WEP, you must enable WEP with 40-bit keys. Use the **set service-profile cipher-wep40** command.

Microsoft Windows XP does not support WEP with WPA. To configure a service profile to provide dynamic WEP for XP clients, leave WPA disabled and use the **set service-profile wep** commands.

To support non-WPA clients that use static WEP, you must configure static WEP keys. Use the **set service-profile wep key-index** command.

Examples — The following command configures service profile *sp2* to use 104-bit WEP encryption:

```
WX4400# set service-profile sp2 cipher-wep104 enable
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile cipher-ccmp** on page 440
- **set service-profile cipher-tkip** on page 441
- **set service-profile cipher-wep40** on page 443
- **set service-profile wep key-index** on page 480
- **set service-profile wpa-ie** on page 481

set service-profile cipher-wep40

Enables dynamic Wired Equivalent Privacy (WEP) with 40-bit keys, in a service profile.

Syntax — `set service-profile name cipher-wep40 {enable | disable}`

- *name* — Service profile name.
- **enable** — Enables 40-bit WEP encryption for WPA clients.
- **disable** — Disables 40-bit WEP encryption for WPA clients.

Defaults — 40-bit WEP encryption is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To use 40-bit WEP with WPA clients, you must also enable the WPA IE.

When 40-bit WEP in WPA is enabled in the service profile, radios managed by a radio profile that is mapped to the service profile can also support non-WPA clients that use dynamic WEP.

To support WPA clients that use 104-bit dynamic WEP, you must enable WEP with 104-bit keys in the service profile. Use the **set service-profile cipher-wep104** command.

Microsoft Windows XP does not support WEP with WPA. To configure a service profile to provide dynamic WEP for XP clients, leave WPA disabled and use the **set service-profile wep** commands.

To support non-WPA clients that use static WEP, you must configure static WEP keys. Use the **set service-profile wep key-index** command.

Examples — The following command configures service profile *sp2* to use 40-bit WEP encryption:

```
WX4400# set service-profile sp2 cipher-wep40 enable
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile cipher-ccmp** on page 440
- **set service-profile cipher-tkip** on page 441
- **set service-profile cipher-wep104** on page 442
- **set service-profile wep key-index** on page 480
- **set service-profile wpa-ie** on page 481

set service-profile cos

Sets the Class-of-Service (CoS) level for static CoS.

Syntax — **set service-profile** *name* **cos** *level*

- **name** — Service profile name.
- **level** — CoS value assigned by the MAP to all traffic in the service profile.

Defaults — The default static CoS level is 0.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — This command applies only when static CoS is enabled. If static CoS is disabled, prioritization is based on the QoS mode configured in the radio profile, and on any ACLs that set CoS. (See the “Configuring Quality of Service” chapter of the *Wireless LAN Switch and Controller Configuration Guide*.) To enable static CoS, use the **set service-profile static-cos** command.

Examples — The following command changes the static CoS level to 7 (voice priority):

```
WX4400# set service-profile sp1 cos 7
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile static-cos** on page 467

set service-profile dhcp-restrict

Enables or disables DHCP Restrict on a service profile. DHCP Restrict filters the traffic from a newly associated client and allows DHCP traffic only, until the client has been authenticated and authorized. All other traffic is captured by the WX and is not forwarded. After the client is successfully authorized, the traffic restriction is removed.

Syntax — `set service-profile name dhcp-restrict {enable | disable}`

- **name** — Service profile name.
- **enable** — Enables DHCP Restrict.
- **disable** — Disables DHCP Restrict.

Examples — DHCP Restrict is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — To further reduce the overhead of DHCP traffic, use the **set service-profile no-broadcast** command to disable DHCP broadcast traffic from MAP radios to clients on the service profile's SSID.

Examples — The following command enables DHCP Restrict on service profile *sp1*:

```
WX4400# set service-profile sp1 dhcp-restrict enable
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile no-broadcast** on page 451
- **set service-profile proxy-arp** on page 452

**set service-profile
idle-client-probing**

Disables or reenables periodic keepalives from MAP radios to clients on a service profile's SSID. When idle-client probing is enabled, the MAP radio sends a unicast null-data frame to each client every 10 seconds. Normally, a client that is still active sends an Ack in reply to the keepalive.

If a client does not send any data or respond to any keepalives before the user idle timeout expires, MSS changes the client session to the Disassociated state.

Syntax — `set service-profile name idle-client-probing {enable | disable}`

- **name** — Service profile name.
- **enable** — Enables keepalives.
- **disable** — Disables keepalives.

Defaults — Idle-client probing is enabled by default.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — The length of time a client can remain idle (unresponsive to idle-client probes) is specified by the **user-idle-timeout** command.

Examples — The following command disables idle-client keepalives on service profile *sp1*:

```
WX4400# set service-profile sp1 idle-client-probing disable  
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile user-idle-timeout** on page 471

set service-profile keep-initial-vlan

Configures MAP radios managed by the radio profile to leave a roamed user on the VLAN assigned by the switch where the user logged on. When this option is disabled, a user's VLAN is reassigned by each WX switch to which a user roams.

Syntax — `set service-profile name keep-initial-vlan {enable | disable}`

- **name** — Service profile name.
- **enable** — Enables radios to leave a roamed user on the same VLAN instead of reassigning the VLAN.
- **disable** — Configures radios to reassign a roamed user's VLAN.

Defaults — This option is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 5.0.

Usage — Even when this option is enabled, the WX switch to which a user roams (the roamed-to switch) can reassign the VLAN in any of the following cases:

- A location policy on the local switch reassigns the VLAN.
- The user is configured in the switch's local database and the VLAN-Name attribute is set on the user or on a user group the user is in.
- The access rule on the roamed-to switch uses RADIUS, and the VLAN-Name attribute is set on the RADIUS server.

Examples — The following command enables the **keep-initial-vlan** option on service profile `sp3`:

```
WX1200# set service-profile sp3 keep-initial-vlan enable
success: change accepted.
```

See Also

- **display service-profile** on page 353

**set service-profile
load-balancing-
exempt**

Exempts a service profile from performing RF load balancing.

Syntax — `set service-profile name load-balancing-exempt {enable | disable}`

- **name** — Service profile name.
- **enable** — Exempts the specified service profile from RF load balancing.
- **disable** — If a service profile has previously been exempted from RF load balancing, restores RF load balancing for the service profile.

Defaults — By default, MAP radios automatically perform RF load balancing for all service profiles.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — Use this command to exempt a service profile from RF load balancing. Exempting a service profile from RF load balancing means that even if an MAP radio is attempting to steer clients away, it does not reduce or conceal the availability of the SSID named in the exempted service profile. Even if a radio is withholding probe responses to manage its load, the radio does respond to probes for an exempt SSID. Also, if an MAP radio is withholding probe responses, and a client probes for *any* SSID, and the radio has at least one exempt SSID, the radio responds to the probe, but the response reveals only the exempt SSID(s).

Examples — The following command exempts service profile *sp3* from RF load balancing:

```
WX# set service-profile sp3 load-balancing-exempt enable
success: change accepted.
```

See Also

- **display load-balancing group** on page 348
- **set load-balancing strictness** on page 399
- **set ap radio load balancing on page 389**
- **set ap local-switching mode** on page 379

**set service-profile
long-retry-count**

Changes the long retry threshold for a service profile. The long retry threshold specifies the number of times a radio can send a long unicast frame without receiving an acknowledgment. A long unicast frame is a frame that is equal to or longer than the frag-threshold.

Syntax — `set service-profile name long-retry-count threshold`

- **name** — Service profile name.
- **threshold** — Number of times the radio can send the same long unicast frame. You can enter a value from 1 through 15.

Defaults — The default long unicast retry threshold is 5 attempts.

Access — *Enabled*.

History — Introduced in MSS Version 4.2.

Examples — The following command changes the long retry threshold for service profile *sp1* to 8:

```
WX4400# set service-profile sp1 long-retry-count 8
success: change accepted.
```

See Also

- **set radio-profile frag-threshold** on page 413
- **set service-profile short-retry-count** on page 456
- **display service-profile** on page 353

**set service-profile
mesh**

Creates a service profile for use with WLAN mesh services.

Syntax — `set service-profile name mesh mode {enable | disable}`

- **name** — Service profile name.
- **enable** — Enables mesh services for the service profile.
- **disable** — Disables mesh services for the service profile.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — Use this command to configure mesh services for a service profile. Once configured, the service profile can then be mapped to a radio profile that manages a radio on the Mesh Portal MAP, which then allows a Mesh Portal AP to beacon a mesh services SSID to Mesh APs.

Examples — The following command enables mesh services for service profile *sp1*:

```
WX# set service-profile sp1 mesh mode enable
success: change accepted.
```

See Also

- **display ap mesh-links** on page 329
- **set ap boot-configuration mesh ssid** on page 373

**set service-profile
no-broadcast**

Disables or reenables the no-broadcast mode. The no-broadcast mode helps reduce traffic overhead on an SSID by having more SSID bandwidth available for unicast traffic. The no-broadcast mode also helps VoIP handsets conserve power by reducing the amount of broadcast traffic sent to the phones.

When enabled, the no-broadcast mode prevents MAP radios from sending DHCP or ARP broadcasts to clients on the service profile's SSID. Instead, a MAP radio handles this traffic as follows:

- ARP requests—If the SSID has clients with IP addresses that the WX does not already know, the WX allows the MAP radio to send the ARP request as a unicast to only those stations whose addresses the WX does not know. The MAP radio does not forward the ARP request as a broadcast and does not send the request as a unicast to stations whose addresses the WX already knows.
- DHCP Offers or Acks—If the destination MAC address belongs to a client on the SSID, the MAP radio sends the DHCP Offer or Ack as a unicast to that client only.

The no-broadcast mode does not affect other types of broadcast traffic and does not prevent clients from sending broadcasts.

Syntax — `set service-profile name no-broadcast {enable | disable}`

- **name** — Service profile name.
- **enable** — Enables the no-broadcast mode. MAP radios are not allowed to send broadcast traffic to clients on the service profile's SSID.
- **disable** — Disables the no-broadcast mode.

Defaults — The no-broadcast mode is disabled by default. (Broadcast traffic not disabled.)

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — To further reduce ARP traffic on a service profile, use the **set service-profile proxy-arp** command to enable Proxy ARP.

Examples — The following command enables the no-broadcast mode on service profile *sp1*:

```
WX4400# set service-profile sp1 no-broadcast enable
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile dhcp-restrict** on page 445
- **set service-profile proxy-arp** on page 452

set service-profile proxy-arp

Enables proxy ARP. When proxy ARP is enabled, the WX replies to ARP requests for client IP address on behalf of the clients. This feature reduces broadcast overhead on a service profile SSID by eliminating ARP broadcasts from MAP radios to the SSID's clients.

If the ARP request is for a client with an IP address the WX does not already know, the WX allows MAP radios to send the ARP request to clients. If the no-broadcast mode is also enabled, the MAP radios send the ARP request as a unicast to only the clients whose addresses the WX does not know. However, if no-broadcast mode is disabled, the MAP radios sends the ARP request as a broadcast to all clients on the SSID.

Syntax — `set service-profile name proxy-arp {enable | disable}`

- **name** — Service profile name.
- **enable** — Enables proxy ARP.
- **disable** — Disables proxy ARP.

Defaults — Proxy ARP is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — To further reduce broadcast traffic on a service profile, use the **set service-profile no-broadcast** command to disable DHCP and ARP request broadcasts.

Examples — The following command enables proxy ARP on service profile *sp1*:

```
WX4400# set service-profile sp1 proxy-arp enable
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile dhcp-restrict** on page 445
- **set service-profile no-broadcast** on page 451

set service-profile psk-phrase

Configures a passphrase for preshared key (PSK) authentication to use for authenticating WPA clients, in a service profile. Radios use the PSK as a pairwise master key (PMK) to derive unique pairwise session keys for individual WPA clients.

Syntax — `set service-profile name psk-phrase passphrase`

- *name* — Service profile name.
- *passphrase* — An ASCII string from 8 to 63 characters long. The string can contain blanks if you use quotation marks at the beginning and end of the string.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — MSS converts the passphrase into a 256-bit binary number for system use and a raw hexadecimal key to store in the WX configuration. Neither the binary number nor the passphrase itself is ever displayed in the configuration.

To use PSK authentication, you must enable it and you also must enable the WPA IE.

Examples — The following command configures service profile *sp3* to use passphrase "1234567890123<>?=&% The quick brown fox jumps over the lazy sl":

```
WX4400# set service-profile sp3 psk-phrase "1234567890123<>
?=&% The quick brown fox jumps over the lazy sl"
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set mac-user attr** on page 261
- **set service-profile auth-psk** on page 435
- **set service-profile psk-raw** on page 454
- **set service-profile wpa-ie** on page 481

set service-profile psk-raw

Configures a raw hexadecimal preshared key (PSK) to use for authenticating WPA clients, in a service profile. Radios use the PSK as a pairwise master key (PMK) to derive unique pairwise session keys for individual WPA clients.

Syntax — `set service-profile name psk-raw hex`

- *name* — Service profile name.
- *hex* — A 64-bit ASCII string representing a 32-digit hexadecimal number. Enter the two-character ASCII form of each hexadecimal number.

Defaults — None.

Examples — Enabled.

History — Introduced in MSS Version 3.0.

Usage — MSS converts the hexadecimal number into a 256-bit binary number for system use. MSS also stores the hexadecimal key in the WX configuration. The binary number is never displayed in the configuration.

To use PSK authentication, you must enable it and you also must enable WPA IE.

Examples — The following command configures service profile *sp3* to use a raw PSK with PSK clients:

```
WX4400# set service-profile sp3 psk-raw c25d3fe4483e867
d1df96eaacdf8b02451fa0836162e758100f5f6b87965e59d
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set mac-user attr** on page 261
- **set service-profile auth-psk** on page 435
- **set service-profile psk-phrase** on page 453
- **set service-profile wpa-ie** on page 481

set service-profile rsn-ie

Enables the Robust Security Network (RSN) Information Element (IE).

The RSN IE advertises the RSN authentication methods and cipher suites supported by radios in the radio profile mapped to the service profile.

Syntax — `set service-profile name rsn-ie {enable | disable}`

- *name* — Service profile name.
- **enable** — Enables the RSN IE.
- **disable** — Disables the RSN IE.

Defaults — The RSN IE is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command enables the RSN IE in service profile *sprsn*:

```
WX4400# set service-profile sprsn rsn-ie enable
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile cipher-ccmp** on page 440

**set service-profile
shared-key-auth**


Enables shared-key authentication, in a service profile.

*Use this command only if advised to do so by 3Com. This command does not enable preshared key (PSK) authentication for Wi-Fi Protected Access (WPA). To enable PSK encryption for WPA, use the **set service-profile auth-psk** command.*

Syntax — `set service-profile name shared-key-auth {enable | disable}`

- `name` — Service profile name.
- `enable` — Enables shared-key authentication.
- `disable` — Disables shared-key authentication.

Defaults — Shared-key authentication is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command enables shared-key authentication in service profile `sp4`:

```
WX4400# set service-profile sp4 shared-key-auth enable
success: change accepted.
```

See Also

- **display radio-profile** on page 350
- **set radio-profile mode** on page 416
- **set service-profile cipher-tkip** on page 441

**set service-profile
short-retry-count**

Changes the short retry threshold for a service profile. The short retry threshold specifies the number of times a radio can send a short unicast frame without receiving an acknowledgment. A short unicast frame is a frame that is shorter than the frag-threshold.

Syntax — `set service-profile name short-retry-count threshold`

- `name` — Service profile name.

- **threshold** — Number of times a radio can send the same short unicast frame. You can enter a value from 1 through 15.

Defaults — The default short unicast retry threshold is 5 attempts.

Examples — Enabled.

History —Introduced in MSS Version 4.2.

Examples — The following command changes the short retry threshold for service profile *sp1* to 3:

```
WX4400# set service-profile sp1 short-retry-count 3
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set radio-profile frag-threshold** on page 413
- **set service-profile long-retry-count** on page 449

set service-profile soda agent-directory

Specifies the directory on the WX where the SODA agent files for a service profile are located.

Syntax — `set service-profile name soda agent-directory directory`

- **name** — Service profile name.
- **directory** — Directory on the WX for SODA agent files.

Defaults — By default, the WX expects SODA agent files to be located in a directory with the same name as SSID.

Access — Enabled.

History —Introduced in MSS Version 4.2.

Usage — If the same SODA agent is used for multiple service profiles, you can use this command to specify a single directory for SODA agent files on the WX, rather than placing the same SODA agent files in a separate directory for each service profile.

Examples — The following command specifies *soda-agent* as the location for SODA agent files for service profile *sp1*:

```
WX4400# set service-profile sp1 soda agent-directory
soda-agent
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **install soda agent** on page 673
- **uninstall soda agent** on page 688

set service-profile soda enforce-checks

Specifies whether a client is allowed access to the network after it has downloaded and run the SODA agent security checks.

Syntax — `set service-profile name soda enforce-checks {enable | disable}`

- **name** — Service profile name.
- **enable** — SODA agent checks are performed before the client is allowed access to the network.
- **disable** — Allows the client access to the network immediately after the SODA agent is downloaded, without waiting for the checks to be run.

Defaults — By default, SODA agent checks are performed before the client is allowed access to the network.

Access — Enabled

History — Introduced in MSS Version 4.2.

Usage — When the SODA agent is enabled in a service profile, by default the SODA agent checks are downloaded to a client and run before the client is allowed on the network. You can use this command to disable the enforcement of the SODA security checks, so that the client is allowed access to the network immediately after the SODA agent is downloaded, rather than waiting for the security checks to be run.

When the enforce checks option is enabled, upon successful completion of the SODA agent checks, the client performs an HTTP Get operation to load the success page. Upon loading the success page, the client is granted access to the network.

In order for the client to load the success page, you must make sure the SODA agent is configured (through SODA Manager) with the correct URL of the success page, so that the WX can serve the page to the client.

Similarly, you must make sure the SODA agent is configured with the correct URLs of the failure and logout pages, so that when the client requests these pages, the WX can serve those pages as well.

Examples — The following command allows network access to clients after they have downloaded the SODA agent, but without requiring that the SODA agent checks be completed:

```
WX4400# set service-profile sp1 soda enforce-checks disable
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile soda mode** on page 462

set service-profile soda failure-page

Specifies a page on the WX that loads when a client fails the security checks performed by the SODA agent.

Syntax — `set service-profile name soda failure-page page`

- **name** — Service profile name.
- **page** — Page that is loaded if the client fails the security checks performed by the SODA agent.

Defaults — By default, the WX dynamically generates a page indicating that the SODA agent checks have failed.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — Use this command to specify a custom page to be loaded by the client when the SODA agent checks fail. After this page is loaded, the specified remediation ACL takes effect, or if there is no remediation ACL configured, then the client is disconnected from the network.

This functionality occurs only when the `enforce checks` option is enabled for the service profile. The `enforce checks` option is enabled by default.

The page is assumed to reside in the root directory on the WX. You can optionally specify a different directory where the page resides.

Examples — The following command specifies *failure.html* as the page to load when a client fails the SODA agent checks:

```
WX4400# set service-profile sp1 soda failure-page
failure.html
success: change accepted.
```

The following command specifies *failure.html*, in the *soda-files* directory, as the page to load when a client fails the SODA agent checks:

```
WX4400# set service-profile sp1 soda failure-page
soda-files/failure.html
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile soda enforce-checks** on page 458
- **set service-profile soda remediation-acl** on page 463

set service-profile soda logout-page

Specifies a page on the WX that is loaded when a client logs out of the network by closing the SODA virtual desktop.

Syntax — `set service-profile name soda logout-page page`

- **name** — Service profile name.
- **page** — Page that is loaded when the client closes the SODA virtual desktop.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 4.2.

Usage — When a client closes the SODA virtual desktop, the client is automatically disconnected from the network. You can use this command to specify a page that loads when the client closes the SODA virtual desktop.

The client can request this page at any time, to ensure that the client's session has been terminated. You can add the IP address of the WX switch to the DNS server as a well-known name, and you can advertise the URL of the page to users as a logout page.

The page is assumed to reside in the root directory on the WX switch. You can optionally specify a different directory where the page resides.

For the logout page to load properly, you must enable the HTTPS server on the WX switch, so that clients can access the page using HTTPS. To do this, use the **set ip https server enable** command.

Examples — The following command specifies *logout.html* as the page to load when a client closes the SODA virtual desktop:

```
WX4400# set service-profile sp1 soda logout-page logout.html
success: change accepted.
```

The following command specifies *logout.html*, in the *soda-files* directory, as the page to load when a client closes the SODA virtual desktop:

```
WX4400# set service-profile sp1 soda logout-page
soda-files/logout.html
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set ip https server** on page 177

**set service-profile
soda mode**

Enables or disables Sygate On-Demand (SODA) functionality for a service profile.

Syntax — `set service-profile name soda mode {enable | disable}`

- **name** — Service profile name.
- **enable** — Enables SODA functionality for the service profile.
- **disable** — Disables SODA functionality for the service profile.

Defaults — Disabled.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — When SODA functionality is enabled for a service profile, a SODA agent is downloaded to clients attempting to connect to a MAP managed by the service profile. The SODA agent performs a series of security-related checks on the client; if the client passes the checks, it can be admitted to the network.

In release 4.2, SODA functionality requires that Web Portal WebAAA also be enabled for the service profile.

Examples — The following command enables SODA functionality for service profile *sp1*:

```
WX4400# set service-profile sp1 soda mode enable
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **install soda agent** on page 673
- **set service-profile soda enforce-checks** on page 458

**set service-profile
soda
remediation-acl**

Specifies an ACL to be applied to a client if it fails the checks performed by the SODA agent.

Syntax — `set service-profile name soda remediation-acl
acl-name`

- **name** — Service profile name.
- **acl-name** — Name of an existing security ACL to use as a remediation ACL for this service profile. ACL names must start with a letter and are case-insensitive.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — If the SODA agent checks fail on a client, by default the client is disconnected from the network. Optionally, you can specify a *failure page* for the client to load (with the **set service-profile soda failure-page** command). When the failure page is loaded, you can optionally specify a *remediation ACL* to apply to the client. The remediation ACL can be used to grant the client limited access to network resources, for example. If there is no remediation ACL configured, then the client is disconnected from the network when the failure page is loaded.

This functionality occurs only when the enforce checks option is enabled for the service profile. The enforce checks option is enabled by default.

Examples — The following command configures the WX to apply *acl-1* to a client when it loads the failure page:

```
WX4400# set service-profile sp1 soda remediation-acl acl-1  
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile soda enforce-checks** on page 458
- **set service-profile soda failure-page** on page 459

**set service-profile
soda success-page**

Specifies a page on the WX that loads when a client passes the security checks performed by the SODA agent.

Syntax — `set service-profile name soda success-page page`

- **name** — Service profile name.
- **page** — Page that is loaded if the client passes the security checks performed by the SODA agent.

Defaults — By default, the WX switch generates a page indicating that the client passed the SODA agent checks.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — Use this command to specify a custom page loaded by the client when it passes the checks performed by the SODA agent. After this page is loaded, the client is placed in its assigned VLAN and granted access to the network.

The page is assumed to reside in the root directory on the WX. You can optionally specify a different directory where the page resides.

This functionality occurs only when the enforce checks option is enabled for the service profile. The enforce checks option is enabled by default.

Examples — The following command specifies *success.html*, which resides in the root directory on the WX, as the page to load when a client passes the SODA agent checks:

```
WX4400# set service-profile sp1 soda success-page  
success.html  
success: change accepted.
```

The following command specifies *success.html*, which resides in the *soda-files* directory on the WX switch, as the page to load when a client passes the SODA agent checks:

```
WX4400# set service-profile sp1 soda success-page  
soda-files/success.html  
success: change accepted.
```


See Also

- **display service-profile** on page 353
- **set service-profile soda enforce-checks** on page 458
- **set service-profile soda mode** on page 462

set service-profile ssid-name

Configures the SSID name in a service profile.

Syntax — `set service-profile name ssid-name ssid-name`

- *name* — Service profile name.
- *ssid-name* — Name of up to 32 alphanumeric characters. You can include blank spaces in the name, if you delimit the name with single or double quotation marks. You must use the same type of quotation mark (either single or double) on both ends of the string.

Defaults — The default SSID name is **private**.

Access — Enabled.

History — Introduced in MSS Version 3.0. Support added for blank spaces in the SSID name in MSS Version 4.0.

Examples — The following command applies the name *guest* to the SSID managed by service profile *clear_wlan*:

```
WX4400# set service-profile clear_wlan ssid-name guest
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile ssid-type** on page 466

**set service-profile
ssid-type**

Specifies whether the SSID managed by a service profile is encrypted or unencrypted.

Syntax — `set service-profile name ssid-type [clear | crypto]`

- *name* — Service profile name.
- **clear** — Wireless traffic for the service profile's SSID is not encrypted.
- **crypto** — Wireless traffic for the service profile's SSID is encrypted.

Defaults — The default SSID type is **crypto**.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command changes the SSID type for service profile *clear_wlan* to **clear**:

```
WX4400# set service-profile clear_wlan ssid-type clear
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile ssid-name** on page 465

**set service-profile
tkip-mc-time**

Changes the length of time that MAP radios use countermeasures if two message integrity code (MIC) failures occur within 60 seconds. When countermeasures are in effect, MAP radios dissociate all TKIP and WPA WEP clients and refuse all association and reassociation requests until the countermeasures end.

Syntax — `set service-profile name tkip-mc-time wait-time`

- *name* — Service profile name.
- *wait-time* — Number of milliseconds (ms) countermeasures remain in effect. You can specify from 0 to 60,000.

Defaults — The default countermeasures wait time is 60,000 ms (60 seconds).

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Countermeasures apply only to TKIP and WEP clients. This includes WPA WEP clients and non-WPA WEP clients. CCMP clients are not affected.

The TKIP cipher suite must be enabled. The WPA IE also must be enabled.

Examples — The following command changes the countermeasures wait time for service profile `sp3` to 30,000 ms (30 seconds):

```
WX4400# set service-profile sp3 tkip-mc-time 30000
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile cipher-tkip** on page 441
- **set service-profile wpa-ie** on page 481

set service-profile static-cos

Enables or disables static CoS on a service profile. Static CoS assigns the same CoS level to all traffic on the service profile's SSID, regardless of 802.1p or DSCP markings in the packets themselves, and regardless of any ACLs that mark CoS. This option provides a simple way to configure an SSID for priority traffic such as VoIP traffic.

When static CoS is enabled, the standard MSS prioritization mechanism is not used. Instead, the MAP sets CoS as follows:

- For traffic from the MAP to clients, the MAP places the traffic into the forwarding queue that corresponds to the CoS level configured on the service profile. For example, if the static CoS level is set to 7, the MAP radio places client traffic in its Voice queue.
- For traffic from clients to the network, the MAP marks the DSCP value in the IP headers of the tunnel packets used to carry the user data from the MAP to the WX switch.

Syntax — `set service-profile name static-cos {enable | disable}`

- **name** — Service profile name.
- **enable** — Enables static CoS on the service profile.
- **disable** — Disables static CoS on the service profile.

Defaults — Static CoS is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — The CoS level is specified by the **set service-profile cos** command.

Examples — The following command enables static CoS on service profile *sp1*:

```
WX4400# set service-profile sp1 static-cos enable
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile cos** on page 444

set service-profile transmit-rates

Changes the data rates supported by MAP radios for a service-profile SSID.

Syntax — **set service-profile** *name* **transmit-rates** {**11a** | **11b** | **11g**} **mandatory** *rate-list* [**disabled** *rate-list*] [**beacon-rate** *rate*] [**multicast-rate** {*rate* | **auto**}]

- *name* — Service profile name.
- **11a** | **11b** | **11g** — Radio type.
- **mandatory** *rate-list* — Set of data transmission rates that clients are required to support in order to associate with an SSID on a MAP radio. A client must support at least one of the mandatory rates.

These rates are advertised in the basic rate set of 802.11 beacons, probe responses, and reassociation response frames sent by MAP radios.

Data frames and management frames sent by MAP radios use one of the specified mandatory rates.

The valid rates depend on the radio type:

- **11a**—6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0
- **11b**—1.0, 2.0, 5.5, 11.0
- **11g**—1.0, 2.0, 5.5, 6.0, 9.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0

Use a comma to separate multiple rates; for example: **6.0,9.0,12.0**

- **disabled** *rate-list* — Data transmission rates that MAP radios do not use to transmit data. This setting applies only to data sent by the MAP radios. The radios still accept frames from clients at disabled data rates.

The valid rates depend on the radio type and are the same as the valid rates for **mandatory**.

- **beacon-rate** *rate* — Data rate of beacon frames sent by MAP radios. This rate is also used for probe-response frames.

The valid rates depend on the radio type and are the same as the valid rates for **mandatory**. However, you cannot set the beacon rate to a disabled rate.

- **multicast-rate** {*rate* | **auto**} — Data rate of multicast frames sent by MAP radios.
 - *rate*—Sets the multicast rate to a specific rate. The valid rates depend on the radio type and are the same as the valid rates for **mandatory**. However, you cannot set the multicast rate to a disabled rate.
 - **auto**—Sets the multicast rate to the highest rate that can reach all clients connected to the MAP radio.

Defaults — This command has the following defaults:

- **mandatory**:
 - 11a—**6.0,12.0,24.0**
 - 11b—**1.0,2.0**
 - 11g—**1.0,2.0,5.5,11.0**
- **disabled**—None. All rates applicable to the radio type are supported by default.

- **beacon-rate:**
 - 11a—**6.0**
 - 11b—**2.0**
 - 11g—**2.0**
- **multicast-rate—auto** for all radio types.

Access — Enabled.

History —Introduced in MSS Version 4.2.

Usage — If you disable a rate, you cannot use the rate as a mandatory rate or the beacon or multicast rate. All rates that are applicable to the radio type and that are not disabled are supported by the radio.

Examples — The following command sets 802.11a mandatory rates for service profile *sp1* to 6 Mbps and 9 Mbps, disables rates 48 Mbps and 54 Mbps, and changes the beacon rate to 9 Mbps:

```
WX4400# set service-profile sp1 transmit-rates 11a mandatory
6.0,9.0 disabled 48.0,54.0 beacon-rate 9.0
success: change accepted.
```

See Also

- **display service-profile** on page 353

set service-profile use-client-dscp

Configures MSS to classify the QoS level of IP packets based on their DSCP value, instead of their 802.11 priority.

Syntax — `set service-profile name user-client-dscp {enable | disable}`

- *name* — Service profile name.
- **enabled** — Enables mapping QoS level from the DSCP level.
- **disabled** — Disables mapping QoS level from the DSCP level.

Defaults — Disabled.

Access — Enabled.

History — Introduced in MSS Version 6.0.

History —If this command is enabled in the service profile, the 802.11 QoS level is ignored, and MSS classifies QoS level of IP packets based on their DSCP value.

Examples — The following command enables mapping the QoS level of IP packets based on their DSCP value for service profile *sp1*:

```
WX# set service-profile sp1 use-client-dscp enable
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **display qos** on page 133

set service-profile user-idle-timeout

Changes the number of seconds MSS leaves a session up for a client that is not sending data and is not responding to keepalives (idle-client probes). If the timer expires, the client session is changed to the Dissociated state.

The timer is reset to 0 each time a client sends data or responds to an idle-client probe. If the idle-client probe is disabled, the timer is reset each time the client sends data.

Syntax — `set service-profile name user-idle-timeout seconds`

- **name** — Service profile name.
- **seconds** — Number of seconds a client is allowed to remain idle before MSS changes the session to the Dissociated state. You can specify from 20 to 86400 seconds.

To disable the timer, specify 0.

Defaults — The default user idle timeout is 180 seconds (3 minutes).

Access — Enabled.

History —Introduced in MSS Version 4.2.

Examples — The following command increases the user idle timeout to 360 seconds (6 minutes):

```
WX4400# set service-profile sp1 user-idle-timeout 360
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile idle-client-probing** on page 446
- **set service-profile web-portal-session-timeout** on page 477

set service-profile web-portal-acl

Changes the ACL name MSS uses to filter Web-Portal user traffic during authentication.

Use this command if you create a custom Web-Portal ACL to allow more than just DHCP traffic during authentication. For example, if you configure an ACL that allows a Web-Portal user to access a credit card server, use this command to use the custom ACL for Web-Portal users that associate with the service profile SSID.

Syntax — `set service-profile name web-portal-acl aclname`

- *name*—Service profile name.
- *aclname*—Name of the ACL to use for filtering Web-Portal user traffic during authentication.

Defaults — By default, a service profile web-portal-acl option is not set. However, when you change the service profile auth-fallthru option to web-portal, MSS sets the web-portal-acl option to *portalacl*. (MSS automatically creates the *portalacl* ACL the first time you set any service profile auth-fallthru option to web-portal.)

Access — Enabled.

History — Introduced in MSS Version 5.0.

Usage — The first time you set the service profile **auth-fallthru** option to **web-portal**, MSS sets the **web-portal-acl** option to *portalacl*. The value remains *portalacl* even if you change the **auth-fallthru** option again. To change the **web-portal-acl** value, you must use the **set service-profile web-portal-acl** command.

The Web-Portal ACL applies only to users who log on using Web Portal, and applies only during authentication. After a Web Portal user is authenticated, the Web Portal ACL no longer applies. ACLs and other user attributes assigned to the username are applied instead.

Examples — The following command changes the Web-Portal ACL name to on service profile *sp3* to *creditsrvr*:

```
WX1200# set service-profile sp3 web-portal-acl creditsrvr
success: change accepted.
```

See Also

- **set service-profile auth-fallthru** on page 434
- **display service-profile** on page 353

set service-profile web-portal-form

Specifies a custom login page that loads for WebAAA users requesting the SSID managed by the service profile.

Syntax — `set service-profile name web-portal-form url`

- *name* — Service profile name.
- *url* — WX subdirectory name and HTML page name of the login page. Specify the full path. For example, *corpa-ssid/corpa.html*.

Defaults — The 3Com Web login page is served by default.

Access — Enabled.

History — Introduced in MSS Version 3.0. Option name changed from **web-aaa-form** to **web-portal-form**, to reflect change to portal-based implementation in MSS Version 4.0.

Usage — 3Com recommends that you create a subdirectory for the custom page and place all the page's files in that subdirectory. Do not place the custom page in the root directory of the switch's user file area.

If the custom login page includes gif or jpg images, their path names are interpreted relative to the directory from which the page is served.



To use WebAAA, the *fallthru* authentication type in the service profile that manages the SSID must be set to **web**. To use WebAAA for a wired authentication port, edit the port configuration with the **set port type wired-auth** command.

Examples — The following commands create a subdirectory named *corpa-ssid*, copy a custom login page named *corpa-login.html* and a jpeg image named *corpa-logo.jpg* into that subdirectory, and set the Web login page for service profile to *corpa-login.html*:

```
WX4400# mkdir corpa-ssid
success: change accepted.
WX4400# copy tftp://10.1.1.1/corpa-login.html corpa-ssid/corpa-login.html
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
WX4400# copy tftp://10.1.1.1/corpa-logo.jpg corpa-ssid/corpa-logo.jpg
success: received 1202 bytes in 0.402 seconds [ 2112 bytes/sec]
WX4400# dir corpa-ssid
=====
file:
Filename                               Size           Created
file:corpa-login.html                  637 bytes     Aug 12 2004, 15:42:26
file:corpa-logo.jpg                    1202 bytes     Aug 12 2004, 15:57:11
Total:          1839 bytes used, 206577 Kbytes free
WX4400# set service-profile corpa-service web-aaa-form corpa-ssid/
corpa-login.html
success: change accepted.
```

See Also

- **copy** on page 667
- **dir** on page 670
- **display service-profile** on page 353
- **mkdir** on page 681
- **set port type wired-auth** on page 100
- **set service-profile auth-fallthru** on page 434
- **set web-portal** on page 278

**set service-profile
web-portal-logout
logout-url**

Specifies the URL that is requested when the user clicks the button to terminate his or her session in the Mobility Domain.

Syntax — `set service-profile profile-name web-portal-logout
logout-url url`

- *name* — Service profile name.
- *url* — Specifies the URL for the Web Portal logout feature. The URL should be of the form **https://host/logout.html**.

Defaults — By default, the logout URL uses the IP address of the WX as the *host* part of the URL. The *host* can be either an IP address or a hostname.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — Specifying the URL for the Web Portal logout feature is useful if you want to standardize the URL across your network. For example, you can configure the logout URL on all of the WX switches in the Mobility Domain as *wifizone.3Com.com/logout.html*, where *wifizone.3Com.com* resolves to one of the WX switches in the Mobility Domain, ideally the seed.

To log out of the network, the user can click the “End Session” button in the pop-under window, or request the logout URL directly.

Standardizing the logout URL serves as a backup means for the user to log out in case the pop-under window is closed inadvertently. Note that if a user requests the logout URL, he or she must enter a username and password in order to identify the session on the WX. (This is not necessary when the user clicks the “End Session” button in the pop-under window.) Both the username and password are required to identify the session. If there is more than one session with the same username, then requesting the logout URL does not end any session.

Examples — The following command configures the Web Portal logout URL as: *wifizone.3Com.com/logout.html* for service profile *sp1*.

```
WX# set service-profile sp1 web-portal-logout logout-url
https://wifizone.3Com.com/logout.html
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile web-portal-logout mode** on page 476

set service-profile web-portal-logout mode

Enables the Web Portal logout functionality, so that a user can manually terminate his or her session.

Syntax — `set service-profile profile-name web-portal-logout mode {enable | disable}`

- *name* — Service profile name.
- **enabled** — Enables the Web Portal logout functionality.
- **disabled** — Disables the Web Portal logout functionality.

Defaults — Disabled.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — When Web Portal logout functionality is enabled, after a Web Portal WebAAA user is successfully authenticated and redirected to the requested page, a pop-under window appears behind the user browser. The window contains a button labeled “End Session”. When the user clicks this button, a URL is requested that terminates the user session in the Mobility Domain.

This feature allows Web Portal users a way to manually log out of the network, instead of waiting to be logged out automatically when the Web Portal WebAAA session timeout period expires.

Examples — The following command enables the Web Portal logout functionality for service profile *sp1*.

```
WX# set service-profile sp1 web-portal-logout mode enable
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile web-portal-logout logout-url** on page 475

set service-profile web-portal-session-timeout

Changes the number of seconds MSS allows Web Portal WebAAA sessions to remain in the Deassociated state before being terminated automatically.

Syntax — `set service-profile name web-portal-session-timeout seconds`

- **name** — Service profile name.
- **seconds** — Number of seconds MSS allows Web Portal WebAAA sessions to remain in the Deassociated state before being terminated automatically. You can specify from 5 to 2800 seconds.

Defaults — The default Web Portal WebAAA session timeout is 5 seconds.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — When a client that has connected through Web Portal WebAAA enters standby or hibernation mode, the client may be idle for longer than the User idle-timeout period. When the User idle-timeout period expires, MSS places the client Web Portal WebAAA session in the Deassociated state. The Web Portal WebAAA session can remain in the Deassociated state for a configurable amount of time before being terminated automatically. This configurable amount of time is called the Web Portal WebAAA session timeout period. You can use this command to set the number of seconds in the Web Portal WebAAA session timeout period.

Note that the Web Portal WebAAA session timeout period applies only to Web Portal WebAAA sessions already authenticated with a username and password. For all other Web Portal WebAAA sessions, the default Web Portal WebAAA session timeout period of 5 seconds is used.

Examples — The following command allows Web Portal WebAAA sessions to remain in the Deassociated state 180 seconds before being terminated automatically.

```
WX4400# set service-profile sp1 web-portal-session-timeout
180
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile user-idle-timeout** on page 471

set service-profile wep active-multicast- index

Specifies the static Wired-Equivalent Privacy (WEP) key (one of four) to use for encrypting multicast frames.

Syntax — **set service-profile**

name **wep active-multicast-index** *num*

- *name* — Service profile name.
- *num* — WEP key number. You can enter a value from 1 through 4.

Defaults — If WEP encryption is enabled and WEP keys are defined, MAP radios use WEP key 1 to encrypt multicast frames, by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Before using this command, you must configure values for the WEP keys you plan to use. Use the **set service-profile wep key-index** command.

Examples — The following command configures service profile *sp2* to use WEP key 2 for encrypting multicast traffic:

```
WX4400# set service-profile sp2 wep active-multicast-index 2
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile wep active-unicast- index** on page 479
- **set service-profile wep key-index** on page 480

**set service-profile
wep active-unicast-
index**

Specifies the static Wired-Equivalent Privacy (WEP) key (one of four) to use for encrypting unicast frames.

Syntax — **set service-profile**

name **wep active-unicast-index** *num*

- *name* — Service profile name.
- *num* — WEP key number. You can enter a value from 1 through 4.

Defaults — If WEP encryption is enabled and WEP keys are defined, MAP radios use WEP key 1 to encrypt unicast frames, by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Before using this command, you must configure values for the WEP keys you plan to use. Use the **set service-profile wep key-index** command.

Examples — The following command configures service profile *sp2* to use WEP key 4 for encrypting unicast traffic:

```
WX4400# set service-profile sp2 wep active-unicast-index 4
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile wep active-multicast- index** on page 478
- **set service-profile wep key-index** on page 480

**set service-profile
wep key-index**

Sets the value of one of four static Wired-Equivalent Privacy (WEP) keys for static WEP encryption.

Syntax — `set service-profile name wep key-index num key value`

- *name* — Service profile name.
- **key-index** *num* — WEP key index. You can enter a value from 1 through 4.
- **key** *value* — Hexadecimal value of the key. You can enter a 10-character ASCII string representing a 5-digit hexadecimal number or a 26-character ASCII string representing a 13-digit hexadecimal number. You can use numbers or letters. ASCII characters in the following ranges are supported:
 - 0 to 9
 - A to F
 - a to f

Defaults — By default, no static WEP keys are defined.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — MSS automatically enables static WEP when you define a WEP key. MSS continues to support dynamic WEP.

If you plan to use static WEP, do not map more than 8 service profiles that contain static WEP keys to the same radio profile.

Examples — The following command configures WEP key index 1 for service profile *sp2* to *aabbccdde*:

```
WX4400# set service-profile sp2 wep key-index 1 key  
aabbccdde  
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile wep active-multicast- index** on page 478
- **set service-profile wep active-unicast- index** on page 479

set service-profile wpa-ie

Enables the WPA information element (IE) in wireless frames. The WPA IE advertises the WPA authentication methods and cipher suites supported by radios in the radio profile mapped to the service profile.

Syntax — `set service-profile name wpa-ie {enable | disable}`

- *name* — Service profile name.
- **enable** — Enables the WPA IE.
- **disable** — Disables the WPA IE.

Defaults — The WPA IE is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — When the WPA IE is enabled, the default authentication method is 802.1X. There is no default cipher suite. You must enable the cipher suites you want the radios to support.

Examples — The following command enables the WPA IE in service profile *sp2*:

```
WX4400# set service-profile sp2 wpa-ie enable
success: change accepted.
```

See Also

- **display service-profile** on page 353
- **set service-profile auth-dot1x** on page 433
- **set service-profile auth-psk** on page 435
- **set service-profile cipher-ccmp** on page 440
- **set service-profile cipher-tkip** on page 441
- **set service-profile cipher-wep104** on page 442
- **set service-profile cipher-wep40** on page 443

12

STP COMMANDS

Use Spanning Tree Protocol (STP) commands to configure and manage spanning trees on the virtual LANs (VLANs) configured on a wireless LAN switch or controller, to maintain a loop-free network.

STP Commands by Usage

This chapter presents STP commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Table 74 STP Commands by Usage

Type	Command
STP State	set spantree on page 501
	display spantree on page 488
	display spantree blockedports on page 492
Bridge Priority	set spantree priority on page 510
Port Cost	set spantree portcost on page 505
	set spantree portvlancost on page 508
	display spantree portvlancost on page 494
	clear spantree portcost on page 484
clear spantree portvlancost on page 485	
Port Priority	set spantree portpri on page 507
	set spantree portvlanpri on page 509
	clear spantree portpri on page 485
	clear spantree portvlanpri on page 486
Timers	set spantree fwddelay on page 503
	set spantree hello on page 503
	set spantree maxage on page 504
Fast Convergence	set spantree portfast on page 506
	display spantree portfast on page 493

Table 74 STP Commands by Usage (continued)

Type	Command
Fast Convergence, cont.	set spantree backbonefast on page 502
	display spantree backbonefast on page 491
	set spantree uplinkfast on page 510
	display spantree uplinkfast on page 500
Statistics	display spantree statistics on page 494
	clear spantree statistics on page 487

clear spantree portcost

Resets to the default value the cost of a network port or ports on paths to the STP root bridge in all VLANs on a WX.

Syntax — `clear spantree portcost port-list`

- *port-list* — List of ports. The port cost is reset on the specified ports.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command resets the cost in all VLANs. To reset the cost for only specific VLANs, use the **clear spantree portvlancost** command.

Examples — The following command resets the STP port cost on ports 5 and 6 to the default value:

```
WX1200# clear spantree portcost 5-6
success: change accepted.
```

See Also

- **clear spantree portvlancost** on page 485
- **display spantree** on page 488
- **display spantree portvlancost** on page 494
- **set spantree portcost** on page 505
- **set spantree portvlancost** on page 508

**clear spantree
portpri**

Resets to the default value the priority of a network port or ports for selection as part of the path to the STP root bridge in all VLANs on a wireless LAN switch or controller.

Syntax — `clear spantree portpri port-list`

- *port-list* — List of ports. The port priority is reset to 32 (the default) on the specified ports.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command resets the priority in all VLANs. To reset the priority for only specific VLANs, use the **clear spantree portvlanpri** command.

Examples — The following command resets the STP priority on port 6 to the default:

```
WX1200# clear spantree portpri 6
success: change accepted.
```

See Also

- **clear spantree portvlanpri** on page 486
- **display spantree** on page 488
- **set spantree portpri** on page 507
- **set spantree portvlanpri** on page 509

**clear spantree
portvlancost**

Resets to the default value the cost of a network port or ports on paths to the STP root bridge for a specific VLAN on a wireless LAN switch, or for all VLANs.

Syntax — `clear spantree portvlancost port-list {all | vlan
vlan-id}`

- *port-list* — List of ports. The port cost is reset on the specified ports.
- **all** — Resets the cost for all VLANs.

- **vlan** *vlan-id* — VLAN name or number. MSS resets the cost for only the specified VLAN.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — MSS does not change a port's cost for VLANs other than the one(s) you specify.

Examples — The following command resets the STP cost for port 2 in VLAN sunflower:

```
WX4400# clear spantree portvlancost 2 vlan sunflower
success: change accepted.
```

See Also

- **clear spantree portcost** on page 484
- **display spantree** on page 488
- **display spantree portvlancost** on page 494
- **set spantree portcost** on page 505
- **set spantree portvlancost** on page 508

clear spantree portvlanpri

Resets to the default value the priority of a network port or ports for selection as part of the path to the STP root bridge, on one VLAN or all VLANs.

Syntax — **clear spantree portvlanpri** *port-list* {**all** | **vlan** *vlan-id*}

- *port-list* — List of ports. The port priority is reset to 32 (the default) on the specified ports.
- **all** — Resets the priority for all VLANs.
- **vlan** *vlan-id* — VLAN name or number. MSS resets the priority for only the specified VLAN.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — MSS does not change a port's priority for VLANs other than the one(s) you specify.

Examples — The following command resets the STP priority for port 2 in VLAN avocado:

```
WX4400# clear spantree portvlanpri 2 vlan avocado
success: change accepted.
```

See Also

- **clear spantree portpri** on page 485
- **display spantree** on page 488
- **set spantree portpri** on page 507
- **set spantree portvlanpri** on page 509

clear spantree statistics

Clears STP statistics counters for a network port or ports and resets them to 0.

Syntax — `clear spantree statistics port-list [vlan vlan-id]`

- *port-list* — List of ports. Statistics counters are reset on the specified ports.
- `vlan vlan-id` — VLAN name or number. MSS resets statistics counters for only the specified VLAN.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command clears STP statistics counters for ports 1, 3, and 5 through 8, for all VLANs:

```
WX1200# clear spantree statistics 1,3,5-8
success: change accepted.
```

See Also

- **display spantree statistics** on page 494

display spantree

Displays STP configuration and port-state information.

Syntax — `display spantree [port-list | vlan vlan-id][active]`

- `port-list` — List of ports. If you do not specify any ports, MSS displays STP information for all ports.
- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, MSS displays STP information for all VLANs.
- `active` — Displays information for only the active (forwarding) ports.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0. Version 4.2 added a value *STP Off* for STP-State and Port-State fields. This state indicates that STP is disabled on the port. The *Disabled* state is still used, but only to indicate that the port is not forwarding traffic.

Examples — The following command displays STP information for VLAN default:

```
WX1200# display spantree vlan default
```

```
VLAN      1
Spanning tree mode          PVST+
Spanning tree type          IEEE
Spanning tree enabled

Designated Root             00-02-4a-70-49-f7
Designated Root Priority     32768
Designated Root Path Cost   19
Designated Root Port        1
Root Max Age 20 sec  Hello Time 2 sec  Forward Delay 15 sec
Bridge ID MAC ADDR          00-0b-0e-02-76-f7
Bridge ID Priority           32768
Bridge Max Age 20 sec  Hello Time 2 sec  Forward Delay 15 sec
```

Port	Vlan	STP-State	Cost	Prio	Portfast
1	1	Forwarding	19	128	Disabled
2	1	STP Off	19	128	Disabled
3	1	Disabled	19	128	Disabled
4	1	Disabled	19	128	Disabled
5	1	Disabled	19	128	Disabled
6	1	Disabled	19	128	Disabled

7	1	Forwarding	19	128	Disabled
8	1	Disabled	19	128	Disabled
9	1	Disabled	19	128	Disabled
17	1	STP Off	19	128	Disabled
18	1	STP Off	19	128	Disabled

Table 75 describes the fields in this display.

Table 75 Output for display spantree

Field	Description
VLAN	VLAN number.
Spanning tree mode	In the current software version, the mode is always <i>PVST+</i> , which means Per VLAN Spanning Tree+.
Spanning tree type	In the current software version, the type is always <i>IEEE 802</i> , which means STP is based on the IEEE 802 standards.
Spanning tree enabled	State of STP on the VLAN.
Designated root	MAC address of the spanning tree's root bridge.
Designated root priority	Bridge priority of the root bridge.
Designated root path cost	Cumulative cost from this bridge to the root bridge. If this WX switch is the root bridge, then the root cost is 0.
Designated root port	Port through which this WX switch reaches the root bridge. If this WX switch is the root bridge, this field says <i>We are the root</i> .
Root max age	Maximum acceptable age for hello packets on the root bridge.
Root hello time	Hello interval on the root bridge.
Root forward delay	Forwarding delay value on the root bridge.
Bridge Id mac addr	This WX switch's MAC address.
Bridge Id priority	This WX switch's bridge priority.
Bridge max age	This WX switch's maximum acceptable age for hello packets.
Bridge hello time	This WX switch's hello interval.
Bridge forward delay	This WX switch's forwarding delay value.

Table 75 Output for display spantree (continued)

Field	Description
Port	Port number. Only network ports are listed. STP does not apply to 3Com Wireless LAN Managed Access Point AP2750 ports or wired authentication ports.
Vlan	VLAN ID.
STP-State or Port-State	STP state of the port: <ul style="list-style-type: none"> ■ Blocking—The port is not forwarding Layer 2 traffic but is listening to and forwarding STP control traffic. ■ Disabled—This state can indicate any of the following conditions: <ul style="list-style-type: none"> ■ The port is inactive. ■ The port is disabled. ■ STP is enabled on the port but the port is not forwarding traffic. (The port is active and enabled but STP has just started to come up.) ■ Forwarding—The port is forwarding Layer 2 traffic. ■ Learning—The port is learning the locations of other devices in the spanning tree before changing state to forwarding. ■ Listening—The port is comparing its own STP information with information in STP control packets received by the port to compute the spanning tree and change state to blocking or forwarding. ■ STP Off—STP is disabled on the port.

Table 75 Output for display spantree (continued)

Field	Description
Port-state	<p>STP state of the port:</p> <ul style="list-style-type: none"> ▪ Blocking — The port is not forwarding Layer 2 traffic but is listening to and forwarding STP control traffic. ▪ Disabled — The port is not forwarding any traffic, including STP control traffic. The port might be administratively disabled or the link might be disconnected. ▪ Forwarding — The port is forwarding Layer 2 traffic. ▪ Learning — The port is learning the locations of other WX switches in the spanning tree before changing state to forwarding. ▪ Listening — The port is comparing its own STP information with information in STP control packets received by the port to compute the spanning tree and change state to blocking or forwarding. ▪ STP Off—STP is disabled on the port.
Cost	STP cost of the port.
Prio	STP priority of the port.
Portfast	<p>State of the uplink fast convergence feature:</p> <ul style="list-style-type: none"> ▪ Enabled ▪ Disabled

See Also

- **display spantree blockedports** on page 492

display spantree backbonefast

Indicates whether the STP backbone fast convergence feature is enabled or disabled.

Syntax — `display spantree backbonefast`

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following example shows the command output on a WX switch with backbone fast convergence enabled:

```
WX4400# display spantree backbonefast
```

```
Backbonefast is enabled
```

See Also

- **set spantree backbonefast** on page 502

display spantree blockedports

Lists information about wireless LAN switch ports that STP has blocked on one or all of its VLANs.

Syntax — `display spantree blockedports [vlan vlan-id]`

- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, MSS displays information for blocked ports on all VLANs.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Usage — The command lists information separately for each VLAN.

Examples — The following command shows information about blocked ports on a WX switch for the default VLAN (VLAN 1):

```
WX4400# display spantree blockedports vlan default
```

Port	Vlan	Port-State	Cost	Prio	Portfast
2	190	Blocking	4	128	Disabled

```
Number of blocked ports (segments) in VLAN 1 : 1
```

The port information is the same as the information displayed by the **display spantree** command. See Table 75 on page 489.

See Also

- **display spantree** on page 488

display spantree portfast

Displays STP uplink fast convergence information for all network ports or for one or more network ports.

Syntax — `display spantree portfast [port-list]`

- `port-list` — List of ports. If you do not specify any ports, MSS displays uplink fast convergence information for all ports.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command shows uplink fast convergence information for all ports:

```
WX1200# display spantree portfast
Port                Vlan  Portfast
-----
1                    1     disable
2                    1     disable
3                    1     disable
4                    1     enable
5                    1     disable
6                    1     disable
7                    1     disable
8                    1     disable
```

Table 76 describes the fields in this display.

Table 76 Output for display spantree portfast

Field	Description
Port	Port number.
VLAN	VLAN number.
Portfast	State of the uplink fast convergence feature: <ul style="list-style-type: none"> ▪ Enable ▪ Disable

See Also

- **set spantree portfast** on page 506

display spantree portvlancost

Shows the cost of a port on a path to the STP root bridge, for each of the port's VLANs.

Syntax — `display spantree portvlancost port-list`

- `port-list` — List of ports.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command shows the STP port cost of port 1:

```
WX4400# display spantree portvlancost 1
port 1 VLAN 1 have path cost 19
```

See Also

- **clear spantree portcost** on page 484
- **clear spantree portvlancost** on page 485
- **display spantree** on page 488
- **set spantree portcost** on page 505
- **set spantree portvlancost** on page 508

display spantree statistics

Displays STP statistics for one or more WX network ports.

Syntax — `display spantree statistics`

`[port-list [vlan vlan-id]]`

- `port-list` — List of ports. If you do not specify any ports, MSS displays STP statistics for all ports.
- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, MSS displays STP statistics for all VLANs.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Usage — The command displays statistics separately for each port.

Examples — The following command shows STP statistics for port 1:

```
WX4400# display spantree statistics 1
```

BPDU related parameters

```
Port 1                VLAN 1
spanning tree enabled for VLAN = 1
port spanning tree    enabled
state                 Forwarding
port_id               0x8015
port_number           0x5
path cost              0x4
message age (port/VLAN) 0(20)
designated_root        00-0b-0e-00-04-30
designated cost        0x0
designated_bridge      00-0b-0e-00-04-30
designated_port        38
top_change_ack        FALSE
config_pending        FALSE
port_inconsistency    none
```

Port based information statistics

```
config BPDU's xmitted(port/VLAN)    0 (1)
config BPDU's received(port/VLAN)    21825 (43649)
tcn BPDU's xmitted(port/VLAN)        0 (0)
tcn BPDU's received(port/VLAN)        2 (2)
forward transition count (port/VLAN)  1 (1)
scp failure count                      0
root inc trans count (port/VLAN)      1 (1)
inhibit loopguard                      FALSE
loop inc trans count                   0 (0)
```

Status of Port Timers

```
forward delay timer                INACTIVE
forward delay timer value           15
message age timer                   ACTIVE
message age timer value              0
topology change timer               INACTIVE
```

```

topology change timer value          0
hold timer                           INACTIVE
hold timer value                      0
delay root port timer                INACTIVE
delay root port timer value          0
delay root port timer restarted is    FALSE

```

VLAN based information & statistics

```

spanning tree type                    ieee
spanning tree multicast address       01-00-0c-cc-cc-cd
bridge priority                       32768
bridge MAC address                    00-0b-0e-12-34-56
bridge hello time                     2
bridge forward delay                  15
topology change initiator:            0
last topology change occurred:        Tue Jul 01 2003 22:33:36.
topology change                       FALSE
topology change time                  35
topology change detected               FALSE
topology change count                 1
topology change last recvd. from      00-0b-0e-02-76-f6

```

Other port specific info

```

dynamic max age transition            0
port BPDU ok count                   21825
msg age expiry count                  0
link loading                          0
BPDU in processing                    FALSE
num of similar BPDU's to process      0
received_inferior_bpdu                FALSE
next state                            0
src MAC count                         21807
total src MAC count                   21825
curr_src_mac                          00-0b-0e-00-04-30
next_src_mac                          00-0b-0e-02-76-f6

```

Table 77 describes the fields in this display.

Table 77 Output for display spantree statistics

Field	Description
Port	Port number.
VLAN	VLAN ID.
Spanning Tree enabled for vlan	State of the STP feature on the VLAN.
port spanning tree state	State of the STP feature on the port. STP state of the port: <ul style="list-style-type: none"> ▪ Blocking — The port is not forwarding Layer 2 traffic but is listening to and forwarding STP control traffic. ▪ Disabled — The port is not forwarding any traffic, including STP control traffic. The port might be administratively disabled or the link might be disconnected. ▪ Forwarding — The port is forwarding Layer 2 traffic. ▪ Learning — The port is learning the locations of other WX switches in the spanning tree before changing state to forwarding. ▪ Listening — The port is comparing its own STP information with information in STP control packets received by the port to compute the spanning tree and change state to blocking or forwarding.
port_id	STP port ID.
port_number	STP port number.
path cost	Cost to use this port to reach the root bridge. This is part of the total path cost (designated cost).
message age	Age of the protocol information for a port and the value of the maximum age parameter (shown in parenthesis) recorded by the switch.
designated_root	MAC address of the root bridge.
designated cost	Total path cost to reach the root bridge.
designated_bridge	Bridge to which this switch forwards traffic away from the root bridge.
designated_port	STP port through which this switch forwards traffic away from the root bridge.
top_change_ack	Value of the topology change acknowledgment flag in the next configured bridge protocol data unit (BPDU) to be transmitted on the associated port. The flag is set in reply to a topology change notification BPDU.

Table 77 Output for display spantree statistics (continued)

Field	Description
config_pending	Indicates whether a configured BPDU is to be transmitted on expiration of the hold timer for the port.
port_inconsistency	Indicates whether the port is in an inconsistent state.
config BPDU's xmitted	Number of BPDUs transmitted from the port. A number in parentheses indicates the number of configured BPDUs transmitted by the WX switch for this VLAN's spanning tree.
config BPDU's received	Number of BPDUs received by this port. A number in parentheses indicates the number of configured BPDUs received by the WX switch for this VLAN's spanning tree.
tcn BPDU's xmitted	Number of topology change notification (TCN) BPDUs transmitted on this port.
tcn BPDU's received	Number of TCN BPDUs received on this port.
forward transition count	Number of times the port state transitioned to the forwarding state.
scp failure count	Number of service control point (SCP) failures.
root inc trans count	Number of times the root bridge changed.
inhibit loopguard	State of the loop guard. In the current release, the state is always FALSE.
loop inc trans count	Number of loops that have occurred.
forward delay timer	Status of the forwarding delay timer. This timer monitors the time spent by a port in the listening and learning states.
forward delay timer value	Current value of the forwarding delay timer, in seconds.
message age timer	Status of the message age timer. This timer measures the age of the received protocol information recorded for a port.
message age timer value	Current value of the message age timer, in seconds.
topology change timer	Status of the topology change timer. This timer determines the time period during which configured BPDUs are transmitted with the topology change flag set by this WX switch when it is the root bridge, after detection of a topology change.
topology change timer value	Current value of the topology change timer, in seconds.

Table 77 Output for display spantree statistics (continued)

Field	Description
hold timer	Status of the hold timer. This timer ensures that configured BPDUs are not transmitted too frequently through any bridge port.
hold timer value	Current value of the hold timer, in seconds.
delay root port timer	Status of the delay root port timer, which enables fast convergence when uplink fast convergence is enabled.
delay root port timer value	Current value of the delay root port timer.
delay root port timer restarted is	Whether the delay root port timer has been restarted.
spanning tree type	Type of spanning tree. The type is always IEEE.
spanning tree multicast address	Destination address used to send out configured BPDUs on a bridge port.
bridge priority	STP priority of this WX switch.
bridge MAC address	MAC address of this WX switch.
bridge hello time	Value of the hello timer interval, in seconds, when this WX switch is the root or is attempting to become the root.
bridge forward delay	Value of the forwarding delay interval, in seconds, when this WX switch is the root or is attempting to become the root.
topology change initiator	Port number that initiated the most recent topology change.
last topology change occurred	System time when the most recent topology change occurred.
topology change	Value of the topology change flag in configuration BPDUs to be transmitted by this WX switch on VLANs for which the switch is the designated bridge.
topology change time	Time period, in seconds, during which BPDUs are transmitted with the topology change flag set by this WX switch when it is the root bridge, after detection of a topology change. It is equal to the sum of the switch's maximum age and forwarding delay parameters.
topology change detected	Indicates whether a topology change has been detected by the switch.
topology change count	Number of times the topology change has occurred.
topology change last recvd. from	MAC address of the bridge from which the WX switch last received a topology change.
dynamic max age transition	Number of times the maximum age parameter was changed dynamically.

Table 77 Output for display spantree statistics (continued)

Field	Description
port BPDU ok count	Number of valid port BPDUs received.
msg age expiry count	Number of expired messages.
link loading	Indicates whether the link is oversubscribed.
BPDU in processing	Indicates whether BPDUs are currently being processed.
num of similar BPDU's to process	Number of similar BPDUs received on a port that need to be processed.
received_inferior_bpdu	Indicates whether the port has received an inferior BPDU or a response to a Root Link Query (RLQ) BPDU.
next state	Port state before it is set by STP.
src MAC count	Number of BPDUs with the same source MAC address.
total src MAC count	Number of BPDUs with all the source MAC addresses.
curr_src_mac	Source MAC address of the current received BPDU.
next_src_mac	Other source MAC address from a different source.

See Also

- **clear spantree statistics** on page 487

display spantree uplinkfast

Shows uplink fast convergence information for one VLAN or all VLANs.

Syntax — `display spantree uplinkfast [vlan vlan-id]`

- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, MSS displays STP statistics for all VLANs.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command shows uplink fast convergence information for all VLANs:

```
WX4400# display spantree uplinkfast
  VLAN      port      list
-----
1           1(fwd),2,3
```

Table 78 describes the fields in this display.

Table 78 Output for display spantree uplinkfast

Field	Description
VLAN	VLAN number.
port list	Ports in the uplink group. The port that is forwarding traffic is indicated by <i>fwd</i> . The other ports are blocking traffic.

See Also

- **set spantree uplinkfast** on page 510

set spantree

Enables or disables STP on one VLAN or all VLANs configured on a WX switch.

Syntax — **set spantree** {**enable** | **disable** }
 [{**all** | **vlan** *vlan-id* | **port** *port-list* *vlan-id* }]

- **enable** — Enables STP.
- **disable** — Disables STP.
- **all** — Enables or disables STP on all VLANs.
- **vlan** *vlan-id* — VLAN name or number. MSS enables or disables STP on only the specified VLAN, on all ports within the VLAN.
- **port** *port-list* *vlan-id* — Port number or list and the VLAN the ports are in. MSS enables or disables STP on only the specified ports, within the specified VLAN.

Defaults — Disabled.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command enables STP on all VLANs configured on a WX switch:

```
WX4400# set spantree enable
success: change accepted.
```

The following command disables STP on VLAN burgundy:

```
WX4400# set spantree disable vlan burgundy
success: change accepted.
```

See Also

- **display spantree** on page 488

**set spantree
backbonefast**

Enables or disables STP backbone fast convergence on a wireless LAN switch. This feature accelerates a port's recovery following the failure of an indirect link.



CAUTION: *The backbone fast convergence feature is not compatible with switches that are running standard IEEE 802.1D Spanning Tree implementations. This includes switches running Rapid Spanning Tree or Multiple Spanning Tree.*

Syntax — `set spantree backbonefast {enable | disable}`

- **enable** — Enables backbone fast convergence.
- **disable** — Disables backbone fast convergence.

Defaults — STP backbone fast path convergence is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — If you plan to use the backbone fast convergence feature, you must enable it on all the bridges in the spanning tree.

Examples — The following command enables backbone fast convergence:

```
WX4400# set spantree backbonefast enable
success: change accepted.
```

See Also

- **display spantree backbonefast** on page 491

**set spantree
fwddelay**

Changes the period of time after a topology change that a WX switch which is not the root bridge waits to begin forwarding Layer 2 traffic on one or all of its configured VLANs. (The root bridge always forwards traffic.)

Syntax — `set spantree fwddelay delay {all | vlan vlan-id}`

- **delay** — Delay value. You can specify from 4 through 30 seconds.
- **all** — Changes the forwarding delay on all VLANs.
- **vlan vlan-id** — VLAN name or number. MSS changes the forwarding delay on only the specified VLAN.

Defaults — The default forwarding delay is 15 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command changes the forwarding delay on VLAN *pink* to 20 seconds:

```
WX4400# set spantree fwddelay 20 vlan pink
success: change accepted.
```

See Also

- **display spantree** on page 488

set spantree hello

Changes the interval between STP hello messages sent by a wireless LAN switch when operating as the root bridge, on one or all of its configured VLANs.

Syntax — `set spantree hello interval {all | vlan vlan-id}`

- **interval** — Interval value. You can specify from 1 through 10 seconds.
- **all** — Changes the interval on all VLANs.
- **vlan vlan-id** — VLAN name or number. MSS changes the interval on only the specified VLAN.

Defaults — The default hello timer interval is 2 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command changes the hello interval for all VLANs to 4 seconds:

```
WX4400# set spantree hello 4 all
success: change accepted.
```

See Also

- **display spantree** on page 488

set spantree maxage

Changes the maximum age for an STP root bridge hello packet that is acceptable to a wireless LAN switch acting as a designated bridge on one or all of its VLANs. After waiting this period of time for a new hello packet, the WX switch determines that the root bridge is unavailable and issues a topology change message.

Syntax — `set spantree maxage aging-time {all | vlan vlan-id}`

- *aging-time* — Maximum age value. You can specify from 6 through 40 seconds.
- **all** — Changes the maximum age on all VLANs.
- **vlan vlan-id** — VLAN name or number. MSS changes the maximum age on only the specified VLAN.

Defaults — The default maximum age for root bridge hello packets is 20 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command changes the maximum acceptable age for root bridge hello packets on all VLANs to 15 seconds:

```
WX4400# set spantree maxage 15 all
success: change accepted.
```

See Also

- **display spantree** on page 488

set spantree portcost

Changes the cost that transmission through a network port or ports in the default VLAN on a wireless LAN switch adds to the total cost of a path to the STP root bridge.

Syntax — `set spantree portcost port-list cost cost`

- *port-list* — List of ports. MSS applies the cost change to all the specified ports.
- **cost cost** — Numeric value. You can specify a value from 1 through 65,535. STP selects lower-cost paths over higher-cost paths.

Defaults — The default port cost depends on the port speed and link type. Table 79 lists the defaults for STP port path cost.

Table 79 SNMP Port Path Cost Defaults

Port Speed	Link Type	Default Port Path Cost
1000 Mbps	Full Duplex Aggregate Link (Port Group)	19
1000 Mbps	Full Duplex	4
100 Mbps	Full Duplex Aggregate Link (Port Group)	19
100 Mbps	Full Duplex	18
100 Mbps	Half Duplex	19
10 Mbps	Full Duplex Aggregate Link (Port Group)	19
10 Mbps	Full Duplex	95
10 Mbps	Half Duplex	100

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command applies only to the default VLAN (VLAN 1). To change the cost of a port in another VLAN, use the **set spantree portvlancost** command.

Examples — The following command changes the cost on ports 3 and 4 to 20:

```
WX1200# set spantree portcost 3,4 cost 20
success: change accepted.
```

See Also

- **clear spantree portcost** on page 484
- **clear spantree portvlancost** on page 485
- **display spantree** on page 488
- **display spantree portvlancost** on page 494
- **set spantree portvlancost** on page 508

set spantree portfast

Enables or disables STP port fast convergence on one or more ports on a wireless LAN switch.

Syntax — `set spantree portfast port port-list {enable | disable}`

- **port *port-list*** — List of ports. MSS enables the feature on the specified ports.
- **enable** — Enables port fast convergence.
- **disable** — Disables port fast convergence.

Defaults — STP port fast convergence is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Use port fast convergence on ports that are directly connected to servers, hosts, or other MAC stations.

Examples — The following command enables port fast convergence on ports 2, 5, and 7:

```
WX1200# set spantree portfast port 2,4,7 enable
success: change accepted.
```

See Also

- **display spantree portfast** on page 493

set spantree portpri Changes the STP priority of a network port or ports for selection as part of the path to the STP root bridge in the default VLAN on a wireless LAN switch.

Syntax — `set spantree portpri port-list priority value`

- *port-list* — List of ports. MSS changes the priority on the specified ports.
- *priority value* — Priority value. You can specify a value from 0 (highest priority) through 255 (lowest priority).

Defaults — The default STP priority for all network ports is 128.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command applies only to the default VLAN (VLAN 1). To change the priority of a port in another VLAN, use the **set spantree portvlanpri** command.

Examples — The following command sets the priority of ports 3 and 4 to 48:

```
WX1200# set spantree portpri 3-4 priority 48
success: change accepted.
```

See Also

- **clear spantree portpri** on page 485
- **clear spantree portvlanpri** on page 486
- **display spantree** on page 488
- **set spantree portvlanpri** on page 509

**set spantree
portvlancost**

Changes the cost of a network port or ports on paths to the STP root bridge for a specific VLAN on a wireless LAN switch.

Syntax — `set spantree portvlancost port-list cost cost {all | vlan vlan-id}`

- `port-list` — List of ports. MSS applies the cost change to all the specified ports.
- `cost cost` — Numeric value. You can specify a value from 1 through 65,535. STP selects lower-cost paths over higher-cost paths.
- `all` — Changes the cost on all VLANs.
- `vlan vlan-id` — VLAN name or number. MSS changes the cost on only the specified VLAN.

Defaults — The default port cost depends on the port speed and link type. (See Table 74 on page 483.)

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command changes the cost on ports 3 and 4 to 20 in VLAN *mauve*:

```
WX1200# set spantree portvlancost 3,4 cost 20 vlan mauve
success: change accepted.
```

See Also

- **clear spantree portcost** on page 484
- **clear spantree portvlancost** on page 485
- **display spantree** on page 488
- **display spantree portvlancost** on page 494
- **set spantree portcost** on page 505

**set spantree
portvlanpri**

Changes the priority of a network port or ports for selection as part of the path to the STP root bridge, on one VLAN or all VLANs.

Syntax — `set spantree portvlanpri`

`port-list priority value {all | vlan vlan-id}`

- `port-list` — List of ports. MSS changes the priority on the specified ports.
- `priority value` — Priority value. You can specify a value from 0 (highest priority) through 255 (lowest priority).
- `all` — Changes the priority on all VLANs.
- `vlan vlan-id` — VLAN name or number. MSS changes the priority on only the specified VLAN.

Defaults — The default STP priority for all network ports is 128.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command sets the priority of ports 3 and 4 to 48 on VLAN *mauve*:

```
WX1200# set spantree portvlanpri 3-4 priority 48 vlan mauve
success: change accepted.
```

See Also

- **clear spantree portpri** on page 485
- **clear spantree portvlanpri** on page 486
- **display spantree** on page 488
- **set spantree portpri** on page 507

**set spantree
priority**

Changes the STP root bridge priority of a wireless LAN switch on one or all of its VLANs.

Syntax — `set spantree priority value {all | vlan vlan-id}`

- **priority value** — Priority value. You can specify a value from 0 through 65,535. The bridge with the lowest priority value is elected to be the root bridge for the spanning tree.
- **all** — Changes the bridge priority on all VLANs.
- **vlan vlan-id** — VLAN name or number. MSS changes the bridge priority on only the specified VLAN.

Defaults — The default root bridge priority for the switch on all VLANs is 32,768.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command sets the bridge priority of VLAN *pink* to 69:

```
WX4400# set spantree priority 69 vlan pink
success: change accepted.
```

See Also

- **display spantree** on page 488

**set spantree
uplinkfast**

Enables or disables STP uplink fast convergence on a wireless LAN switch. This feature enables a WX switch with redundant links to the network backbone to immediately switch to the backup link to the root bridge if the primary link fails.

Syntax — `set spantree uplinkfast {enable | disable}`

- **enable** — Enables uplink fast convergence.
- **disable** — Disables uplink fast convergence.

Defaults — Disabled.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — The uplink fast convergence feature is applicable to bridges that are acting as access switches to the network core (distribution layer) but are not in the core themselves. Do not enable the feature on WX switches that are in the network core.

Examples — The following command enables uplink fast convergence:

```
WX4400# set spantree uplinkfast enable  
success: change accepted.
```

See Also

- **display spantree uplinkfast** on page 500

13

IGMP SNOOPING COMMANDS

Use Internet Group Management Protocol (IGMP) snooping commands to configure and manage multicast traffic reduction on a WX.

Commands by usage

This chapter presents IGMP snooping commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Table 80 IGMP Commands by Usage

Type	Command
IGMP Snooping State	set igmp on page 525
	display igmp on page 514
Proxy Reporting	set igmp proxy-report on page 530
Pseudo-querier	set igmp querier on page 533
	display igmp querier on page 519
Timers	set igmp qi on page 531
	set igmp oqi on page 529
	set igmp qri on page 532
	set igmp lmqi on page 526
	set igmp rv on page 534
Router Solicitation	set igmp mrsol on page 528
	set igmp mrsol mrsi on page 528
Multicast Routers	set igmp mrouter on page 527
	display igmp mrouter on page 518
Multicast Receivers	set igmp receiver on page 533
	display igmp receiver-table on page 521
Statistics	display igmp statistics on page 523
	clear igmp statistics on page 514

clear igmp statistics Clears IGMP statistics counters on one VLAN or all VLANs on a wireless LAN switch and resets them to 0.

Syntax — `clear igmp statistics [vlan vlan-id]`

- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, IGMP statistics are cleared for all VLANs.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command clears IGMP statistics for all VLANs:

```
WX1200# clear igmp statistics
IGMP statistics cleared for all vlans
```

See Also — [display igmp statistics](#) on page 523

display igmp Displays IGMP configuration information and statistics.

Syntax — `display igmp [vlan vlan-id]`

- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, MSS displays IGMP information for all VLANs.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays IGMP information for VLAN *orange*:

```
WX1200# display igmp vlan orange
VLAN: orange
IGMP is enabled
Proxy reporting is on
Mrouter solicitation is on
Querier functionality is off
Configuration values: qi: 125 oqi: 300 qri: 100 lmqi: 10 rvalue: 2 Multicast
router information:
Port Mrouter-IPaddr Mrouter-MAC          Type  TTL
-----
  1      192.28.7.5 00:01:02:03:04:05 dvmrp  17
Group      Port Receiver-IP      Receiver-MAC      TTL
-----
      224.0.0.2 none                none                none undef
237.255.255.255 5      10.10.10.11 00:02:04:06:08:0b 258
237.255.255.255 5      10.10.10.13 00:02:04:06:08:0d 258
237.255.255.255 5      10.10.10.14 00:02:04:06:08:0e 258
237.255.255.255 5      10.10.10.12 00:02:04:06:08:0c 258
237.255.255.255 5      10.10.10.10 00:02:04:06:08:0a 258
Querier information:
Querier for vlan orange
Port Querier-IP      Querier-MAC          TTL
-----
  1 193.122.135.178 00:0b:cc:d2:e9:b4    23
IGMP vlan member ports: 1, 2, 3
IGMP static ports: none
IGMP statistics for vlan orange:

IGMP message type Received Transmitted Dropped
-----
General-Queries      0          0          0
GS-Queries           0          0          0
Report V1            0          0          0
Report V2            5          1          4
Leave                 0          0          0
Mrouter-Adv          0          0          0
Mrouter-Term         0          0          0
Mrouter-Sol          50         101         0
DVMRP                4          4          0
PIM V1               0          0          0
PIM V2               0          0          0
Topology notifications: 0
Packets with unknown IGMP type: 0
Packets with bad length: 0
Packets with bad checksum: 0
Packets dropped: 4
```

Table 81 describes the fields in this display.

Table 81 Output for display igmp

Field	Description
VLAN	VLAN name. MSS displays information separately for each VLAN.
IGMP is enabled (disabled)	IGMP state.
Proxy reporting	Proxy reporting state.
Mrouter solicitation	Multicast router solicitation state.
Querier functionality	Pseudo-querier state.
Configuration values (qi)	Query interval.
Configuration values (oqi)	Other-querier-present interval.
Configuration values (qri)	Query response interval.
Configuration values (lmqi)	Last member query interval.
Configuration values (rvalue)	Robustness value.
Multicast router information	List of multicast routers and active multicast groups. The fields containing this information are described separately. The display igmp mrouter command shows the same information.
Port	Number of the physical port through which the WX can reach the router.
Mrouter-IPaddr	IP address of the multicast router interface.
Mrouter-MAC	MAC address of the multicast router interface.
Type	How the WX learned that the port is a multicast router port: <ul style="list-style-type: none"> ▪ conf — Static multicast port configured by an administrator ▪ madv — Multicast advertisement ▪ quer — IGMP query ▪ dvmrp — Distance Vector Multicast Routing Protocol (DVMRP) ▪ pimv1 — Protocol Independent Multicast (PIM) version 1 ▪ pimv2 — PIM version 2

Table 81 Output for display igmp (continued)

Field	Description
TTL	Number of seconds before this entry ages out if not refreshed. For static multicast router entries, the time-to-live (TTL) value is <i>undef</i> . Static multicast router entries do not age out.
Group	IP address of a multicast group. The display igmp receiver-table command shows the same information as these receiver fields.
Port	Physical port through which the WX can reach the group's receiver.
Receiver-IP	IP address of the client receiving the group.
Receiver-MAC	MAC address of the client receiving the group.
TTL	Number of seconds before this entry ages out if the WX does not receive a group membership message from the receiver. For static multicast receiver entries, the TTL value is <i>undef</i> . Static multicast receiver entries do not age out.
Querier information	Information about the subnet's multicast querier. If the querier is another WX switch, the fields described below are applicable. If the querier is the WX itself, the output indicates how many seconds remain until the next general query message. If IGMP snooping does not detect a querier, the output indicates this. The display igmp querier command shows the same information.
Querier for vlan	VLAN containing the querier. Information is listed separately for each VLAN.
Querier-IP	IP address of the querier.
Querier-MAC	MAC address of the querier.
TTL	Number of seconds before this entry ages out if the WX does not receive a query message from the querier.
IGMP vlan member ports	Physical ports in the VLAN. This list includes all network ports configured to be in the VLAN and all ports MSS dynamically assigns to the VLAN when a user assigned to the VLAN becomes a receiver. For example, the list can include a MAP access port that is not configured to be in the VLAN when a user associated with the 3Com Wireless LAN Managed Access Point AP2750 on that port becomes a receiver for a group. When all receivers on a dynamically added port age out, MSS removes the port from the list.
IGMP static ports	Static receiver ports.
IGMP statistics	Multicast message and packet statistics. These are the same statistics displayed by the display igmp statistics command.

Table 81 Output for display igmp (continued)

Field	Description
VLAN	VLAN name. MSS displays information separately for each VLAN.
IGMP is enabled (disabled)	IGMP state.

See Also

- **display igmp mrouter** on page 518
- **display igmp querier** on page 519
- **display igmp receiver-table** on page 521
- **display igmp statistics** on page 523

display igmp mrouter

Displays the multicast routers in a WX's subnet, on one VLAN or all VLANs. Routers are listed separately for each VLAN, according to the port number through which the wireless LAN switch can reach the router.

Syntax — `display igmp mrouter [vlan vlan-id]`

- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, MSS displays the multicast routers in all VLANs.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays the multicast routers in VLAN *orange*:

```
WX1200# display igmp mrouter vlan orange
Multicast routers for vlan orange
Port Mrouter-IPaddr  Mrouter-MAC          Type  TTL
-----
  1      192.28.7.5  00:01:02:03:04:05  dvmrp  33
```

Table 82 describes the fields in this display.

Table 82 Output for display igmp mrouter

Field	Description
Multicast routers for vlan	VLAN containing the multicast routers. Ports are listed separately for each VLAN.
Port	Number of the physical port through which the WX can reach the router.
Mrouter-IPAddr	IP address of the multicast router.
Mrouter-MAC	MAC address of the multicast router.
Type	How the WX learned that the port is a multicast router port: <ul style="list-style-type: none"> ▪ conf — Static multicast port configured by an administrator ▪ madv — Multicast advertisement ▪ quer — IGMP query ▪ dvmrp — Distance Vector Multicast Routing Protocol (DVMRP) ▪ pimv1 — Protocol Independent Multicast (PIM) version 1 ▪ pimv2 — PIM version 2
TTL	Number of seconds before this entry ages out if unused. For static multicast router entries, the TTL value is <i>undef</i> . Static multicast router entries do not age out.

See Also

- **display igmp mrouter** on page 518
- **set igmp mrouter** on page 527

display igmp querier

Shows information about the active multicast querier, on one VLAN or all VLANs. Queriers are listed separately for each VLAN. Each VLAN can have only one querier.

Syntax — `display igmp querier [vlan vlan-id]`

- **vlan vlan-id** — VLAN name or number. If you do not specify a VLAN, MSS displays querier information for all VLANs.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command displays querier information for VLAN *orange*:

```
WX1200# display igmp querier vlan orange
Querier for vlan orange
Port Querier-IP      Querier-MAC      TTL
-----
  1 193.122.135.178 00:0b:cc:d2:e9:b4  23
```

The following command shows the information MSS displays when the querier is the WX itself:

```
WX1200# display igmp querier vlan default
Querier for vlan default:
I am the querier for vlan default, time to next query is 20
```

The output indicates how many seconds remain before the pseudo-querier on the WX switch broadcasts the next general query report to IP address 224.0.0.1, the multicast all-systems group.

If IGMP snooping does not detect a querier, the output indicates this finding, as shown in the following example:

```
WX1200# display igmp querier vlan red
Querier for vlan red:
There is no querier present on vlan red
```

This condition does not necessarily indicate a problem. For example, election of the querier might be in progress.

Table 83 describes the fields in this display. Table 82 on page 519 describes the fields in the display when a querier other than the WX is present.

Table 83 Output for display igmp mrouter

Field	Description
Querier for vlan	VLAN containing the querier. Information is listed separately for each VLAN.
Querier-IP	IP address of the querier interface.
Querier-MAC	MAC address of the querier interface.
TTL	Number of seconds before this entry ages out if the WX does not receive a query message from the querier.

See Also

- **set igmp querier** on page 533

display igmp receiver-table

Displays the receivers to which a WX forwards multicast traffic. You can display receivers for all VLANs, a single VLAN, or a group or groups identified by group address and network mask.

Syntax — **display igmp receiver-table** [**vlan** *vlan-id*] [**group** *group-ip-addr/mask-length*]

- **vlan** *vlan-id* — VLAN name or number. If you do not specify a VLAN, MSS displays the multicast receivers on all VLANs.
- **group** *group-ip-addr/mask-length* — IP address and subnet mask of a multicast group, in CIDR format (for example, 239.20.20.10/24). If you do not specify a group address, MSS displays the multicast receivers for all groups.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays all multicast receivers in VLAN *orange*:

```
WX1200# display igmp receiver-table vlan orange
VLAN: orange
Session          Port Receiver-IP      Receiver-MAC      TTL
-----
      224.0.0.2  none           none              none  undef
237.255.255.255  5      10.10.10.11  00:02:04:06:08:0b  179
237.255.255.255  5      10.10.10.13  00:02:04:06:08:0d  179
237.255.255.255  5      10.10.10.14  00:02:04:06:08:0e  179
237.255.255.255  5      10.10.10.12  00:02:04:06:08:0c  179
237.255.255.255  5      10.10.10.10  00:02:04:06:08:0a  179
```

The following command lists all receivers for multicast groups 237.255.255.1 through 237.255.255.255, in all VLANs:

```
WX1200# display igmp receiver-table group 237.255.255.0/24
VLAN: red
Session          Port Receiver-IP      Receiver-MAC      TTL
-----
237.255.255.2    2     10.10.20.19 00:02:04:06:09:0d 112
237.255.255.119  3     10.10.30.31 00:02:04:06:01:0b 112

VLAN: green
Session          Port Receiver-IP      Receiver-MAC      TTL
-----
237.255.255.17   1     10.10.40.41 00:02:06:08:02:0c  12
237.255.255.255  6     10.10.60.61 00:05:09:0c:0a:01 111
```

Table 84 describes the fields in this display.

Table 84 Output for display igmp receiver-table

Field	Description
VLAN	VLAN that contains the multicast receiver ports. Ports are listed separately for each VLAN.
Session	IP address of the multicast group being received.
Port	Physical port through which the WX can reach the receiver.
Receiver-IP	IP address of the receiver.
Receiver-MAC	MAC address of the receiver.
TTL	Number of seconds before this entry ages out if the WX does not receive a group membership message from the receiver. For static multicast receiver entries, the TTL value is <i>undef</i> . Static multicast receiver entries do not age out.

See Also

- **set igmp receiver** on page 533

display igmp statistics

Shows IGMP statistics.

Syntax — `display igmp statistics [vlan vlan-id]`

- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, MSS displays IGMP statistics for all VLANs.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays IGMP statistics for VLAN *orange*:

```
WX1200# display igmp statistics vlan orange
IGMP statistics for vlan orange:
```

```
IGMP message type Received Transmitted Dropped
-----
General-Queries          0           0           0
GS-Queries                0           0           0
Report V1                 0           0           0
Report V2                 5           1           4
Leave                      0           0           0
Mrouter-Adv               0           0           0
Mrouter-Term              0           0           0
Mrouter-Sol               50          101          0
DVMRP                     4           4           0
PIM V1                    0           0           0
PIM V2                     0           0           0
Topology notifications: 0
Packets with unknown IGMP type: 0
Packets with bad length: 0
Packets with bad checksum: 0
Packets dropped: 4
```

Table 85 describes the fields in this display.

Table 85 Output of display igmp statistics

Field	Description
IGMP statistics for vlan	VLAN name. Statistics are listed separately for each VLAN.
IGMP message type	Type of IGMP message: <ul style="list-style-type: none"> ■ General-Queries — General group membership queries sent by the multicast querier (multicast router or pseudo-querier). ■ GS-Queries — Group-specific queries sent by the multicast querier to determine whether there are receivers for a specific group. ■ Report V1 — IGMP version 1 group membership reports sent by clients who want to be receivers for the groups. ■ Report V2 — IGMP version 2 group membership reports sent by clients who want to be receivers for the groups. ■ Leave — IGMP version 2 leave messages sent by clients who want to stop receiving traffic for a group. Leave messages apply only to IGMP version 2. ■ Mrouter-Adv — Multicast router advertisement packets. A multicast router sends this type of packet to advertise the IP address of the sending interface as a multicast router interface. ■ Mrouter-Term — Multicast router termination messages. A multicast router sends this type of message when multicast forwarding is disabled on the router interface, the router interface is administratively disabled, or the router itself is gracefully shutdown. ■ Mrouter-Sol — Multicast router solicitation messages. A multicast client or a WX sends this type of message to immediately solicit multicast router advertisement messages from the multicast routers in the subnet. ■ DVMRP — Distance Vector Multicast Routing Protocol (DVMRP) messages. Multicast routers running DVMRP exchange multicast information with these messages. ■ PIM V1 — Protocol Independent Multicast (PIM) version 1 messages. Multicast routers running PIMv1 exchange multicast information with these messages. ■ PIM V2 — PIM version 2 messages.
Received	Number of packets received.
Transmitted	Number of packets transmitted. This number includes both multicast packets originated by the WX and multicast packets received and then forwarded by the WX.
Dropped	Number of IGMP packets dropped by the WX.

Table 85 Output of display igmp statistics (continued)

Field	Description
Topology notifications	Number of Layer 2 topology change notifications received by the WX. In the current software version, the value in this field is always 0.
Packets with unknown IGMP type	Number of multicast packets received with an unrecognized multicast type.
Packets with bad length	Number of packets with an invalid length.
Packets with bad IGMP checksum	Number of packets with an invalid IGMP checksum value.
Packets dropped	Number of multicast packets dropped by the WX.

See Also

- **clear igmp statistics** on page 514

set igmp

Disables or reenables IGMP snooping on one VLAN or all VLANs on a wireless LAN switch.

Syntax — `set igmp {enable | disable} [vlan vlan-id]`

- **enable** — Enables IGMP snooping.
- **disable** — Disables IGMP snooping.
- **vlan *vlan-id*** — VLAN name or number. If you do not specify a VLAN, IGMP snooping is disabled or reenabled on all VLANs.

History — Introduced in MSS Version 3.0.

Examples — The following command disables IGMP snooping on VLAN *orange*:

```
WX1200# set igmp disable vlan orange
success: change accepted
```

See Also

- **set igmp rv** on page 534

set igmp lmqi

Changes the IGMP last member query interval timer on one VLAN or all VLANs on a wireless LAN switch.

Syntax — `set igmp lmqi tenth-seconds [vlan vlan-id]`

- **lmqi *tenth-seconds*** — Amount of time (in tenths of a second) that the WX waits for a response to a group-specific query after receiving a leave message for that group, before removing the receiver that sent the leave message from the list of receivers for the group. If there are no more receivers for the group, the WX switch also sends a leave message for the group to multicast routers. You can specify a value from 1 through 65,535.
- **vlan *vlan-id*** — VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults — The default last member query interval is 10 tenths of a second (1 second).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command changes the last member query interval on VLAN *orange* to 5 tenths of a second:

```
WX1200# set igmp lmqi 5 vlan orange
success: change accepted.
```

See Also

- **set igmp oqi** on page 529
- **set igmp qi** on page 531
- **set igmp mrouter** on page 527

set igmp mrouter

Adds or removes a port in a WX's list of ports on which it forwards traffic to multicast routers. Static multicast ports are immediately added to or removed from the list of router ports and do not age out.

Syntax — `set igmp mrouter port port-list {enable | disable}`

- **port** *port-list* — Port list. MSS adds or removes the specified ports in the list of static multicast router ports.
- **enable** — Adds the port to the list of static multicast router ports.
- **disable** — Removes the port from the list of static multicast router ports.

Defaults — By default, no ports are static multicast router ports.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You cannot add MAP access ports or wired authentication ports as static multicast ports. However, MSS can dynamically add these port types to the list of multicast ports based on multicast traffic.

Examples — The following command adds port 6 as a static multicast router port:

```
WX1200# set igmp mrouter port 6 enable
success: change accepted.
```

The following command removes port 6 from the static multicast router port list:

```
WX1200# set igmp mrouter port 6 disable
success: change accepted.
```

See Also

- **display igmp statistics** on page 523

set igmp mrsol

Enables or disables multicast router solicitation by a WX.

Syntax — `set igmp mrsol {enable | disable} [vlan vlan-id]`

- **enable** — Enables multicast router solicitation.
- **disable** — Disables multicast router solicitation.
- **vlan *vlan-id*** — VLAN name or number. If you do not specify a VLAN, multicast router solicitation is disabled or enabled on all VLANs.

Defaults — Multicast router solicitation is disabled on all VLANs by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command enables multicast router solicitation on VLAN *orange*:

```
WX1200# set igmp mrsol enable vlan orange
success: change accepted
```

See Also

- **set igmp mrsol mrsi** on page 528

set igmp mrsol mrsi

Changes the interval between multicast router solicitations by a WX on one VLAN or all VLANs.

Syntax — `set igmp mrsol mrsi seconds [vlan vlan-id]`

- **seconds** — Number of seconds between multicast router solicitations. You can specify a value from 1 through 65,535.
- **vlan *vlan-id*** — VLAN name or number. If you do not specify a VLAN, MSS changes the multicast router solicitation interval for all VLANs.

Defaults — The interval between multicast router solicitations is 30 seconds by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You cannot add MAP access ports or wired authentication ports as static multicast ports. However, MSS can dynamically add these port types to the list of multicast ports based on multicast traffic.

Examples — The following example changes the multicast router solicitation interval to 60 seconds:

```
WX1200# set igmp mrsol mrsi 60
success: change accepted.
```

See Also

- **set igmp mrsol** on page 528.

set igmp oqi

Changes the IGMP other-querier-present interval timer on one VLAN or all VLANs on a WX.

Syntax — `set igmp oqi seconds [vlan vlan-id]`

- `oqi seconds` — Number of seconds that the WX waits for a general query to arrive before electing itself the querier. You can specify a value from 1 through 65,535.
- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults — The default other-querier-present interval is 255 seconds (4.25 minutes).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — A WX cannot become the querier unless the pseudo-querier feature is enabled on the WX switch. When the feature is enabled, the WX becomes the querier for a subnet so long as the WX does not receive a query message from a router with a lower IP address than the IP address of the WX in that subnet. To enable the pseudo-querier feature, use **set igmp querier**.

Examples — The following command changes the other-querier-present interval on VLAN *orange* to 200 seconds:

```
WX1200# set igmp oqi 200 vlan orange
success: change accepted.
```

See Also

- **set igmp lmqi** on page 526
- **set igmp qi** on page 531
- **set igmp qri** on page 532
- **set igmp querier** on page 533
- **set igmp mrouter** on page 527
- **set igmp rv** on page 534

**set igmp
proxy-report**

Disables or reenables proxy reporting by a WX on one VLAN or all VLANs.

Syntax — `set igmp proxy-report {enable | disable}`

- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, proxy reporting is disabled or reenabled on all VLANs.
- `enable` — Enables proxy reporting.
- `disable` — Disables proxy reporting.

Defaults — Proxy reporting is enabled on all VLANs by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Proxy reporting reduces multicast overhead by sending only one membership report for a group to the multicast routers and discarding other membership reports for the same group. If you disable proxy reporting, the WX sends all membership reports to the routers, including multiple reports for the same group.

Examples — The following example disables proxy reporting on VLAN *orange*:

```
WX1200# set igmp proxy-report disable vlan orange
success: change accepted.
```

See Also

- **set igmp rv** on page 534

set igmp qi

Changes the IGMP query interval timer on one VLAN or all VLANs on a WX.

Syntax — `set igmp qi seconds [vlan vlan-id]`

- `qi seconds` — Number of seconds that elapse between general queries sent by the WX when the WX switch is the querier for the subnet. You can specify a value from 1 through 65,535.
- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults — The default query interval is 125 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The query interval is applicable only when the WX is querier for the subnet. For the WX switch to become the querier, the pseudo-querier feature must be enabled on the WX and the WX must have the lowest IP address among all the WX switches eligible to become a querier. To enable the pseudo-querier feature, use the **set igmp querier** command.

Examples — The following command changes the query interval on VLAN *orange* to 100 seconds:

```
WX1200# set igmp qi 100 vlan orange
success: change accepted.
```

See Also

- **set igmp lmqi** on page 526
- **set igmp oqi** on page 529
- **set igmp qri** on page 532
- **set igmp querier** on page 533
- **set igmp mrouter** on page 527
- **set igmp rv** on page 534

set igmp qri

Changes the IGMP query response interval timer on one VLAN or all VLANs on a WX.

Syntax — `set igmp qri tenth-seconds [vlan vlan-id]`

- **qri *tenth-seconds*** — Amount of time (in tenths of a second) that the WX waits for a receiver to respond to a group-specific query message before removing the receiver from the receiver list for the group. You can specify a value from 1 through 65,535.
- **vlan *vlan-id*** — VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults — The default query response interval is 100 tenths of a second (10 seconds).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The query response interval is applicable only when the WX is querier for the subnet. For the WX to become the querier, the pseudo-querier feature must be enabled on the WX and the WX must have the lowest IP address among all the WX switches eligible to become a querier. To enable the pseudo-querier feature, use **set igmp querier**.

Examples — The following command changes the query response interval on VLAN *orange* to 50 tenths of a second (5 seconds):

```
WX1200# set igmp qri 50 vlan orange
success: change accepted.
```

See Also

- **set igmp lmqi** on page 526
- **set igmp oqi** on page 529
- **set igmp qi** on page 531
- **set igmp querier** on page 533
- **set igmp rv** on page 534

set igmp querier

Enables or disables the IGMP pseudo-querier on a WX, on one VLAN or all VLANs.

Syntax — `set igmp querier {enable | disable} [vlan vlan-id]`

- **enable** — Enables the pseudo-querier.
- **disable** — Disables the pseudo-querier.
- **vlan *vlan-id*** — VLAN name or number. If you do not specify a VLAN, the pseudo-querier is enabled or disabled on all VLANs.

Defaults — The pseudo-querier is disabled on all VLANs by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — 3Com recommends that you use the pseudo-querier only when the VLAN contains local multicast traffic sources and no multicast router is servicing the subnet.

Examples — The following example enables the pseudo-querier on the *orange* VLAN:

```
WX1200# set igmp querier enable vlan orange
success: change accepted.
```

See Also

- **display igmp querier** on page 519

set igmp receiver

Adds or removes a network port in the list of ports on which a WX forwards traffic to multicast receivers. Static multicast receiver ports are immediately added to or removed from the list of receiver ports and do not age out.

Syntax — `set igmp receiver port port-list {enable | disable}`

- **port *port-list*** — Network port list. MSS adds the specified ports to the list of static multicast receiver ports.
- **enable** — Adds the port to the list of static multicast receiver ports.
- **disable** — Removes the port from the list of static multicast receiver ports.

Defaults — By default, no ports are static multicast receiver ports.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You cannot add MAP access ports or wired authentication ports as static multicast ports. However, MSS can dynamically add these port types to the list of multicast ports based on multicast traffic.

Examples — The following command adds port 7 as a static multicast receiver port:

```
WX1200# set igmp receiver port 7 enable
success: change accepted.
```

The following command removes port 7 from the list of static multicast receiver ports:

```
WX1200# set igmp receiver port 7 disable
success: change accepted.
```

See Also

- **display igmp receiver-table** on page 521

set igmp rv

Changes the robustness value for one VLAN or all VLANs on a WX. Robustness adjusts the IGMP timers to the amount of traffic loss that occurs on the network.

Syntax — `set igmp rv num [vlan vlan-id]`

- *num* — Robustness value. You can specify a value from 2 through 255. Set the robustness value higher to adjust for more traffic loss.
- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, MSS changes the robustness value for all VLANs.

Defaults — The default robustness value for all VLANs is 2.

Access — Enabled.

History — Introduced in MSS Version 3.0.

See Also

- **set igmp oqi** on page 529
- **set igmp qi** on page 531
- **set igmp qri** on page 532

14

SECURITY ACL COMMANDS

Use security ACL commands to configure and monitor security access control lists (ACLs). Security ACLs filter packets to restrict or permit network usage by certain users or traffic types, and can assign to packets a class of service (CoS) to define the priority of treatment for packet filtering.

(Security ACLs are different from the location policy on a WX, which helps you locally control user access. For location policy commands, see “AAA Commands” on page 211.)

Security ACL Commands by Usage

This chapter presents security ACL commands alphabetically. Use Table 86 to locate commands in this chapter based on their use.

Table 86 Security ACL Commands by Usage

Type	Command
Create Security ACLs	set security acl on page 552
	display security acl editbuffer on page 543
	display security acl on page 542
	display security acl info on page 545
Commit Security ACLs	clear security acl on page 538
	commit security acl on page 541
Map Security ACLs	rollback security acl on page 551
	set security acl map on page 557
	display security acl map on page 546
Monitor Security ACLs	clear security acl map on page 539
	display security acl hits on page 544
	set security acl hit-sample-rate on page 559
	display security acl resource-usage on page 547

clear security acl

Clears a specified security ACL, an access control entry (ACE), or all security ACLs, from the edit buffer. When used with the command **commit security acl**, clears the ACE from the running configuration.

Syntax — **clear security acl** {*acl-name* | **all**} [*editbuffer-index*]

- *acl-name* — Name of an existing security ACL to clear. ACL names start with a letter and are case-insensitive.
- **all** — Clears all security ACLs.
- *editbuffer-index* — Number that indicates which access control entry (ACE) in the security ACL to clear. If you do not specify an ACE, all ACEs are cleared from the ACL.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command deletes security ACLs only in the edit buffer. You must use the **commit security acl** command with this command to delete the ACL or ACE from the running configuration and nonvolatile storage.

The **clear security acl** command deletes a security ACL, but does not stop its current filtering function if the ACL is mapped to any virtual LANs (VLANs), ports, or virtual ports, or if the ACL is applied in a Filter-Id attribute to an authenticated user or group of users with current sessions.

Examples — The following commands display the current security ACL configuration, *clear acl_133* in the edit buffer, commit the deletion to the running configuration, and redisplay the ACL configuration to display that it no longer contains *acl_133*:

```

WX4400# display security acl info all
ACL information for all
set security acl ip acl_133 (hits #1 0)
-----
1. deny IP source IP 192.168.1.6 0.0.0.0 destination IP any
set security acl ip acl_134 (hits #3 0)
-----
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
set security acl ip acl_135 (hits #2 0)
-----
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits
WX4400# clear security acl acl_133
WX4400# commit security acl acl_133
configuration accepted
WX4400# display security acl info all
ACL information for all
set security acl ip acl_134 (hits #3 0)
-----
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
set security acl ip acl_135 (hits #2 0)
-----
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits

```

See Also

- **clear security acl map** on page 539
- **commit security acl** on page 541
- **display security acl info** on page 545
- **set security acl** on page 552

clear security acl map

Deletes the mapping between a security ACL and a virtual LAN (VLAN), one or more physical ports, or a virtual port. Or deletes all ACL maps to VLANs, ports, and virtual ports on a WX switch.



*Security ACLs are applied to users or groups dynamically via the Filter-Id attribute. To delete a security ACL from a user or group in the local WX database, use the command **clear user attr**, **clear mac-user attr**, **clear usergroup attr**, or **clear mac-usergroup attr**. To delete a security ACL from a user or group on an external RADIUS server, see the documentation for your RADIUS server.*

Syntax — `clear security acl map {acl-name | all} {vlan vlan-id | port port-list [tag tag-value] | ap ap-num} {in | out}`

- `acl-name` — Name of an existing security ACL to clear. ACL names start with a letter and are case-insensitive.
- `all` — Removes security ACL mapping from all physical ports, virtual ports, and VLANs on a WX switch.
- `vlan vlan-id` — VLAN name or number. MSS removes the security ACL from the specified VLAN.
- `port port-list` — Port list. MSS removes the security ACL from the specified WX physical port or ports.
- `tag tag-value` — Tag value that identifies a virtual port in a VLAN. Specify a value from 1 through 4095. MSS removes the security ACL from the specified virtual port.
- `ap ap-num` — One or more MAPs, based on their connection IDs. Specify a single connection ID, or specify a comma-separated list of connection IDs, a hyphen-separated range, or any combination, with no spaces. MSS removes the security ACL from the specified MAPs.
- `in` — Removes the security ACL from traffic coming *into* the WX switch.
- `out` — Removes the security ACL from traffic going *out of* the WX switch.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To clear a security ACL map, type the name of the ACL with the VLAN, physical port or ports, virtual port tag, or Distributed MAP and the direction of the packets to stop filtering. This command deletes the ACL mapping, but not the ACL.

Examples — To clear the mapping of security ACL `acljoe` from port 4 for incoming packets, type the following command:

```
WX4400# clear security acl map acljoe port 4 in
clear mapping accepted
```

To clear all physical ports, virtual ports, and VLANs on a WX switch of the ACLs mapped for incoming and outgoing traffic, type the following command:

```
WX4400# clear security acl map all
success: change accepted.
```

See Also

- **clear security acl** on page 538
- **display security acl map** on page 546
- **set security acl map** on page 557

commit security acl

Saves a security ACL, or all security ACLs, in the edit buffer to the running configuration and nonvolatile storage on the WX switch. Or, when used with the clear security acl command, **commit security acl** deletes a security ACL, or all security ACLs, from the running configuration and nonvolatile storage.

Syntax — **commit security acl** {*acl-name* | **all**}

- *acl-name* — Name of an existing security ACL to commit. ACL names must start with a letter and are case-insensitive.
- **all** — Commits all security ACLs in the edit buffer.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Use the **commit security acl** command to save security ACLs into, or delete them from, the permanent configuration. Until you commit the creation or deletion of a security ACL, it is stored in an edit buffer and is not enforced. After you commit a security ACL, it is removed from the edit buffer.

A single **commit security acl all** command commits the creation and/or deletion of whatever **display security acl info all editbuffer** shows to be currently stored in the edit buffer.

Examples — The following commands commit all the security ACLs in the edit buffer to the configuration, display a summary of the committed ACLs, and show that the edit buffer has been cleared:

```
WX4400# commit security acl all
configuration accepted
WX4400# display security acl
ACL table
ACL                               Type   Class   Mapping
-----
acl_123                            IP     Static
acl_124                            IP     Static
WX4400# display security acl info all editbuffer
acl editbuffer information for all
```

See Also

- **clear security acl** on page 538
- **display security acl** on page 542
- **display security acl info** on page 545
- **rollback security acl** on page 551
- **set security acl** on page 552

display security acl

Displays a summary of the security ACS that are mapped.

Syntax — `display security acl`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command lists only the ACLs that have been mapped to something (a user, or VLAN, or port, and so on). To list all committed ACLs, use the **display security acl info** command. To list ACLs that have not yet been committed, use the **display security acl editbuffer** command.

Examples — To display a summary of the mapped security ACLs on a on a WX switch, type the following command:

```

WX4400# display security acl
ACL table
ACL                               Type Class Mapping
-----
acl_123                           IP    Static Port 2 In
acl_133                           IP    Static Port 4 In
acl_124                           IP    Static

```

See Also

- **clear security acl** on page 538
- **display security acl info** on page 545
- **display security acl editbuffer** on page 543
- **set security acl** on page 552

display security acl editbuffer

Displays a summary of the security ACLs that have not yet been committed to the configuration.

Syntax — `display security acl [info all] editbuffer`

- *info all* — Displays the ACEs in each uncommitted ACL. Without this option, only the ACE names are listed.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 1.0.

Examples — To view a summary of the security ACLs in the edit buffer, type the following command:

```

WX4400# display security acl editbuffer
ACL edit-buffer table
ACL                               Type Status
-----
acl_111                           IP    Not committed
acl-a                              IP    Not committed

```

To view details about these uncommitted ACLs, type the following command.

```
WX4400# display security acl info all editbuffer
ACL edit-buffer information for all
set security acl ip acl-111 (ACEs 3, add 3, del 0,
modified 2)
-----
 1. permit IP source IP 192.168.254.12 0.0.0.0 destination IP
any
 2. permit IP source IP 192.168.253.11 0.0.0.0 destination IP
any
 3. deny SRC source IP 192.168.253.1 0.0.0.255
set security acl ip acl-a (ACEs 1, add 1, del 0, modified 0)
-----
 1. permit SRC source IP 192.168.1.1 0.0.0.0
```

See Also

- **clear security acl** on page 538
- **commit security acl** on page 541
- **display security acl** on page 542
- **display security acl info** on page 545
- **set security acl** on page 552

display security acl hits

Displays the number of packets filtered by security ACLs (“hits”) on the WX switch. Each time a packet is filtered by a security ACL, the hit counter increments.

Syntax — `display security acl hits`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — For MSS to count hits for a security ACL, you must specify hits in the **set security acl** commands that define ACE rules for the ACL.

Examples — To display the security ACL hits on a WX switch, type the following command:

```
WX4400# display security acl hits
ACL hit-counters
Index Counter          ACL-name
-----
      1              0 acl_2
      2              0 acl_175
      3             916 acl_123
```

See Also

- **set security acl hit-sample-rate** on page 559
- **set security acl** on page 552

display security acl info

Displays the contents of a specified security ACL or all security ACLs that are committed — saved in the running configuration and nonvolatile storage — or the contents of security ACLs in the edit buffer before they are committed.

Syntax — `display security acl info {acl-name | all} [editbuffer]`

- *acl-name* — Name of an existing security ACL to display. ACL names must start with a letter and are case-insensitive.
- **all** — Displays the contents of all security ACLs.
- **editbuffer** — Displays the contents of the specified security ACL or all security ACLs that are stored in the edit buffer after being created with **set security acl**. If you do not use this parameter, only committed ACLs are shown.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. The *acl-name* | **all** option is no longer required; **display security acl info** is valid and displays the same information as **security acl info all** in MSS Version 4.1.

Examples — To display the contents of all security ACLs committed on a WX switch, type the following command:

```
WX4400# display security acl info
ACL information for all
set security acl ip acl_123 (hits #5 462)
-----
1. permit IP source IP 192.168.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 192.168.2.11 0.0.0.0 destination IP any
set security acl ip acl_134 (hits #3 0)
-----
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
set security acl ip acl_135 (hits #2 0)
-----
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits
```

The following command displays the contents of *acl_123* in the edit buffer, including the committed ACE rules 1 and 2 and the uncommitted rule 3:

```
WX4400# display security acl info acl_123 editbuffer
ACL edit-buffer information for acl_123
set security acl ip acl_123 (ACEs 3, add 3, del 0, modified 0)
-----
1. permit IP source IP 192.168.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 192.168.2.11 0.0.0.0 destination IP any
3. deny SRC source IP 192.168.1.234 255.255.255.255 enable-hits
```

See Also

- **clear security acl** on page 538
- **commit security acl** on page 541
- **set security acl** on page 552

display security acl map

Displays the VLANs, ports, and virtual ports on the WX switch to which a security ACL is assigned.

Syntax — `display security acl map acl-name`

- *acl-name* — Name of an existing security ACL for which to show static mapping. ACL names must start with a letter and are case-insensitive.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command displays the port to which security ACL *acl_111* is mapped:

```
WX4400# display security acl map acl_111
ACL acl_111 is mapped to:
Port 4 in
```

See Also

- **clear security acl map** on page 539
- **display security acl map** on page 546
- **set security acl map** on page 557

display security acl resource-usage

Displays statistics about the resources used by security ACL filtering on the WX switch.

Syntax — `display security acl resource-usage`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Use this command with the help of 3Com to diagnose an ACL resource problem. (To obtain 3Com Technical Support, see “Obtaining Support for Your 3Com Products” on page 739.)

Examples — To display security ACL resource usage, type the following command:

```
WX4400# display security acl resource-usage
ACL resources

Classifier tree counters
-----
Number of rules           : 2
Number of leaf nodes     : 1
Stored rule count        : 2
Leaf chain count         : 1
Longest leaf chain       : 2
Number of non-leaf nodes : 0
Uncompressed Rule Count  : 2
Maximum node depth      : 1
Sub-chain count          : 0
PSCBs in primary memory  : 0 (max: 512)
PSCBs in secondary memory : 0 (max: 9728)
Leaves in primary        : 2 (max: 151)
Leaves in secondary      : 0 (max 12096)
Sum node depth           : 1

Information on Network Processor status
-----
Fragmentation control    : 0
UC switchdest            : 0

ACL resources
Port number              : 0
Number of action types   : 2
LUdef in use             : 5
Default action pointer   : c8007dc
L4 global                : True
No rules                 : False
Non-IP rules             : False
Root in first            : True
Static default action    : False
No per-user (MAC) mapping : True
Out mapping              : False
In mapping               : True
No VLAN or PORT mapping  : False
No VPORT mapping        : True
```

Table 87 explains the fields in the **display security acl resource-usage** output.

Table 87 Output of display security acl resource-usage

Field	Description
Number of rules	Number of security ACEs currently mapped to ports or VLANs.
Number of leaf nodes	Number of security ACL data entries stored in the rule tree.
Stored rule count	Number of security ACEs stored in the rule tree.
Leaf chain count	Number of chained security ACL data entries stored in the rule tree.
Longest leaf chain	Longest chain of security ACL data entries stored in the rule tree.
Number of non-leaf nodes	Number of nodes with no data entries stored in the rule tree.
Uncompressed Rule Count	Number of security ACEs stored in the rule tree, including duplicates—ACEs in ACLs applied to multiple ports, virtual ports, or VLANs.
Maximum node depth	Number of data elements in the rule tree, from the root to the furthest data entry (leaf).
Sub-chain count	Sum of action types represented in all security ACL data entries.
PSCBs in primary memory	Number of pattern search control blocks (PSCBs) stored in primary node memory.
PSCBs in secondary memory	Number of PSCBs stored in secondary node memory.
Leaves in primary	Number of security ACL data entries stored in primary leaf memory.
Leaves in secondary	Number of ACL data entries stored in secondary leaf memory.
Sum node depth	Total number of security ACL data entries.
Fragmentation control	Control value for handling fragmented IP packets. Note: The current MSS version filters only the first packet of a fragmented IP packet and passes the remaining fragments.
UC switchdest	Control value for handling fragmented IP packets. Note: The current MSS version filters only the first packet of a fragmented IP packet and passes the remaining fragments.
Port number	Control value for handling fragmented IP packets. Note: The current MSS version filters only the first packet of a fragmented IP packet and passes the remaining fragments.
Number of action types	Number of actions that can be performed by ACLs. This value is always 2, because ACLs can either <i>permit</i> or <i>deny</i> .

Table 87 Output of display security acl resource-usage (continued)

Field	Description
LUdef in use	Number of the lookup definition (LUdef) table currently in use for packet handling.
Default action pointer	Memory address used for packet handling, from which default action data is obtained when necessary.
L4 global	Security ACL mapping on the WX switch: <ul style="list-style-type: none"> ▪ True — Security ACLs are mapped. ▪ False — No security ACLs are mapped.
No rules	Security ACE rule mapping on the WX switch: <ul style="list-style-type: none"> ▪ True — No security ACEs are mapped. ▪ False — Security ACEs are mapped.
Non-IP rules	Non-IP security ACE mapping on the WX switch: <ul style="list-style-type: none"> ▪ True — Non-IP security ACEs are mapped. ▪ False — Only IP security ACEs are mapped. <p>Note: The current MSS version supports security ACEs for IP only.</p>
Root in first	Leaf buffer allocation: <ul style="list-style-type: none"> ▪ True — Enough primary leaf buffers are allocated in nonvolatile memory to accommodate all leaves. ▪ False — Insufficient primary leaf buffers are allocated in nonvolatile memory to accommodate all leaves.
Static default action	Definition of a default action: <ul style="list-style-type: none"> ▪ True — A default action types is defined. ▪ False — No default action type is defined.
No per-user (MAC) mapping	Per-user application of a security ACL with the Filter-Id attribute, on the WX switch: <ul style="list-style-type: none"> ▪ True — No security ACLs are applied to users. ▪ False — Security ACLs are applied to users.
Out mapping	Application of security ACLs to outgoing traffic on the WX switch: <ul style="list-style-type: none"> ▪ True — Security ACLs are mapped to outgoing traffic. ▪ False — No security ACLs are mapped to outgoing traffic.

Table 87 Output of display security acl resource-usage (continued)

Field	Description
In mapping	<p>Application of security ACLs to incoming traffic on the WX switch:</p> <ul style="list-style-type: none"> ▪ True — Security ACLs are mapped to incoming traffic. ▪ False — No security ACLs are mapped to incoming traffic.
No VLAN or PORT mapping	<p>Application of security ACLs to WX VLANs or ports on the WX switch:</p> <ul style="list-style-type: none"> ▪ True — No security ACLs are mapped to VLANs or ports. ▪ False — Security ACLs are mapped to VLANs or ports.
No VPORT mapping	<p>Application of security ACLs to WX virtual ports on the WX switch:</p> <ul style="list-style-type: none"> ▪ True — No security ACLs are mapped to virtual ports. ▪ False — Security ACLs are mapped to virtual ports.

rollback security acl

Clears changes made to the security ACL edit buffer since it was last saved. The ACL is rolled back to its state after the last **commit security acl** command was entered. All uncommitted ACLs in the edit buffer are cleared.

Syntax — **rollback security acl** {*acl-name* | **all**}

- *acl-name* — Name of an existing security ACL to roll back. ACL names must start with a letter and are case-insensitive.
- **all** — Rolls back all security ACLs in the edit buffer, clearing all uncommitted ACEs.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following commands show the edit buffer before a rollback, clear any changes in the edit buffer to *security acl_122*, and show the edit buffer after the rollback:

```
WX4400# display security acl info all editbuffer
ACL edit-buffer information for all
set security acl ip acl_122 (ACEs 3, add 3, del 0, modified 0)
-----
1. permit IP source IP 20.0.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 20.0.2.11 0.0.0.0 destination IP any
3. deny SRC source IP 192.168.1.234 255.255.255.255 enable-hits
WX4400# rollback security acl acl_122
WX4400# display security acl info all editbuffer
ACL edit-buffer information for all
```

See Also

- **display security acl** on page 542

set security acl

In the edit buffer, creates a security access control list (ACL), adds one access control entry (ACE) to a security ACL, and/or reorders ACEs in the ACL. The ACEs in an ACL filter IP packets by source IP address, a Layer 4 protocol, or IP, ICMP, TCP, or UDP packet information.

By source address

Syntax — **set security acl ip** *acl-name* {**permit** [**cos** *cos*] | **deny**} *source-ip-addr mask* [**before editbuffer-index** | **modify editbuffer-index**] [**hits**]

By Layer 4 protocol

Syntax — **set security acl ip** *acl-name* {**permit** [**cos** *cos*] | **deny**} *protocol-number* {*source-ip-addr mask destination-ip-addr mask*} [**precedence** *precedence*] [**tos** *tos*] [**before editbuffer-index** | **modify editbuffer-index**] [**hits**]

By IP packets

Syntax — **set security acl ip** *acl-name* {**permit** [**cos** *cos*] | **deny**} **ip** {*source-ip-addr mask destination-ip-addr mask*} [**precedence** *precedence*] [**tos** *tos*] [**before editbuffer-index** | **modify editbuffer-index**] [**hits**]

By ICMP packets

Syntax — `set security acl ip acl-name {permit [cos cos] | deny} icmp {source-ip-addr mask destination-ip-addr mask [type icmp-type] [code icmp-code] [precedence precedence] [tos tos] [before editbuffer-index | modify editbuffer-index] [hits]}`

By TCP packets

Syntax — `set security acl ip acl-name {permit [cos cos] | deny} tcp {source-ip-addr mask [operator port [port2]] destination-ip-addr mask [operator port [port2]]} [precedence precedence] [tos tos] [established] [before editbuffer-index | modify editbuffer-index] [hits]}`

By UDP packets

Syntax — `set security acl ip acl-name {permit [cos cos] | deny} udp {source-ip-addr mask [operator port [port2]] destination-ip-addr mask [operator port [port2]]} [precedence precedence] [tos tos] [before editbuffer-index | modify editbuffer-index] [hits]}`

- *acl-name* — Security ACL name. ACL names must be unique within the WX switch, must start with a letter, and are case-insensitive. Specify an ACL name of up to 32 of the following characters:
 - Letters a through z and A through Z
 - Numbers 0 through 9
 - Hyphen (-), underscore (_), and period (.)

3Com recommends that you do not use the same name with different capitalizations for ACLs. For example, do not configure two separate ACLs with the names *acl_123* and *ACL_123*.



*In an ACL name, do not include the term **all**, **default-action**, **map**, **help**, or **editbuffer**.*

- **permit** — Allows traffic that matches the conditions in the ACE.
- **cos cos** — For permitted packets, a class-of-service (CoS) level for packet handling. Specify a value from 0 through 7:
 - 1 or 2—Background. Packets are queued in MAP forwarding queue 4.

- 0 or 3—Best effort. Packets are queued in MAP forwarding queue 3.
- 4 or 5—Video. Packets are queued in MAP forwarding queue 2. Use CoS level 4 or 5 for voice over IP (VoIP) packets other than SpectraLink Voice Priority (SVP).
- 6 or 7—Voice. Packets are queued in MAP forwarding queue 1. In MSS Version 3.0, use 6 or 7 only for VoIP phones that use SVP, not for other types of traffic.
- **deny** — Blocks traffic that matches the conditions in the ACE.
- *protocol* — IP protocol by which to filter packets:
 - **ip**
 - **tcp**
 - **udp**
 - **icmp**
 - A protocol number between 0 and 255.

(For a complete list of IP protocol names and numbers, see www.iana.org/assignments/protocol-numbers.)

- *source-ip-addr mask* — IP address and wildcard mask of the network or host from which the packet is being sent. Specify both address and mask in dotted decimal notation. For more information, see “Wildcard Masks” on page 30.
- *operator port [port2]* — Operand and port number(s) for matching TCP or UDP packets to the number of the source or destination port on source-ip-addr or destination-ip-addr. Specify one of the following operands and the associated port:
 - **eq** — Packets are filtered for only *port* number.
 - **gt** — Packets are filtered for all ports that are greater than *port* number.
 - **lt** — Packets are filtered for all ports that are less than *port* number.
 - **neq** — Packets are filtered for all ports except *port* number.
 - **range** — Packets are filtered for ports in the range between *port* and *port2*. To specify a port range, enter two port numbers. Enter the lower port number first, followed by the higher port number.

(For a complete list of TCP and UDP port numbers, see www.iana.org/assignments/port-numbers.)

- *destination-ip-addr mask* — IP address and wildcard mask of the network or host to which the packet is being sent. Specify both address and mask in dotted decimal notation. For more information, see “Wildcard Masks” on page 30.
- **type** *icmp-type* — Filters ICMP messages by type. Specify a value from 0 through 255. (For a list of ICMP message type and code numbers, see www.iana.org/assignments/icmp-parameters.)
- **code** *icmp-code* — For ICMP messages filtered by type, additionally filters ICMP messages by code. Specify a value from 0 through 255. (For a list of ICMP message type and code numbers, see www.iana.org/assignments/icmp-parameters.)
- **precedence** *precedence* — Filters packets by precedence level. Specify a value from 0 through 7:
 - 0 — routine precedence
 - 1 — priority precedence
 - 2 — immediate precedence
 - 3 — flash precedence
 - 4 — flash override precedence
 - 5 — critical precedence
 - 6 — internetwork control precedence
 - 7 — network control precedence
- **tos** *tos* — Filters packets by type of service (TOS) level. Specify one of the following values, or any sum of these values up to 15. For example, a **tos** value of **9** filters packets with the TOS levels minimum delay (**8**) and minimum monetary cost (**1**).
 - 8 — minimum delay
 - 4 — maximum throughput
 - 2 — maximum reliability
 - 1 — minimum monetary cost
 - 0 — normal
- **established** — For TCP packets only, applies the ACE only to established TCP sessions and not to new TCP sessions.

- **before** *editbuffer-index* — Inserts the new ACE in front of another ACE in the security ACL. Specify the number of the existing ACE in the edit buffer. Index numbers start at 1. (To display the edit buffer, use **display security acl editbuffer**.)
- **modify** *editbuffer-index* — Replaces an ACE in the security ACL with the new ACE. Specify the number of the existing ACE in the edit buffer. Index numbers start at 1. (To display the edit buffer, use **display security acl editbuffer**.)
- **hits** — Tracks the number of packets that are filtered based on a security ACL, for all mappings.

Defaults — Permitted packets are assigned to class-of-service (CoS) class 0 by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The WX switch does not apply security ACLs until you activate them with the **commit security acl** command and map them to a VLAN, port, or virtual port, or to a user. If the WX switch is reset or restarted, any ACLs in the edit buffer are lost.

You cannot perform ACL functions that include permitting, denying, or marking with a Class of Service (CoS) level on packets with a multicast or broadcast destination address.

The order of security ACEs in a security ACL is important. Once an ACL is active, its ACEs are checked according to their order in the ACL. If an ACE criterion is met, its action takes place and any ACEs that follow are ignored.

ACEs are listed in the order in which you create them, unless you move them. To position security ACEs within a security ACL, use **before editbuffer-index** and **modify editbuffer-index**.

Examples — The following command adds an ACE to security *acl_123* that permits packets from IP address 192.168.1.11/24 and counts the hits:

```
WX4400# set security acl ip acl_123 permit
192.168.1.11 0.0.0.255 hits
```

The following command adds an ACE to `acl_123` that denies packets from IP address 192.168.2.11:

```
WX4400# set security acl ip acl_123 deny 192.168.2.11
0.0.0.0
```

The following command creates `acl_125` by defining an ACE that denies TCP packets from source IP address 192.168.0.1 to destination IP address 192.168.0.2 for established sessions only, and counts the hits:

```
WX4400# set security acl ip acl_125 deny tcp
192.168.0.1 0.0.0.0 192.168.0.2 0.0.0.0 established hits
```

The following command adds an ACE to `acl_125` that denies TCP packets from source IP address 192.168.1.1 to destination IP address 192.168.1.2, on destination port 80 only, and counts the hits:

```
WX4400# set security acl ip acl_125 deny tcp
192.168.1.1 0.0.0.0 192.168.1.2 0.0.0.0 eq 80 hits
```

Finally, the following command commits the security ACLs in the edit buffer to the configuration:

```
WX4400# commit security acl all
configuration accepted
```

See Also

- **clear security acl** on page 538
- **commit security acl** on page 541
- **display security acl** on page 542

set security acl map

Assigns a committed security ACL to a VLAN, physical port or ports, virtual port, or Distributed MAP on the WX switch.



*To assign a security ACL to a user or group in the local WX database, use the command **set user attr**, **set mac-user attr**, **set usergroup attr**, or **set mac-usergroup attr** with the `Filter-Id` attribute. To assign a security ACL to a user or group with `Filter-Id` on a RADIUS server, see the documentation for your RADIUS server.*

Syntax — `set security acl map acl-name {vlan vlan-id | port port-list [tag tag-list] | ap ap-num} {in | out}`

- *acl-name* — Name of an existing security ACL to map. ACL names start with a letter and are case-insensitive.
- **vlan** *vlan-id* — VLAN name or number. MSS assigns the security ACL to the specified VLAN.
- **port** *port-list* — Port list. MSS assigns the security ACL to the specified physical WX port or ports.
- **tag** *tag-list* — One or more values that identify a virtual port in a VLAN. Specify a single tag value from 1 through 4095. Or specify a comma-separated list of values, a hyphen-separated range, or any combination, with no spaces. MSS assigns the security ACL to the specified virtual port or ports.
- **ap** *ap-num* — One or more MAPs, based on their connection IDs. Specify a single connection ID, or specify a comma-separated list of connection IDs, a hyphen-separated range, or any combination, with no spaces. MSS assigns the security ACL to the specified MAPs.
- **in** — Assigns the security ACL to traffic coming *into* the WX switch.
- **out** — Assigns the security ACL to traffic coming *from* the WX switch.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Before you can map a security ACL, you must use the **commit security acl** command to save the ACL in the running configuration and nonvolatile storage.

For best results, map only one input security ACL and one output security ACL to each VLAN, physical port, virtual port, or Distributed MAP to filter a flow of packets. If more than one security ACL filters the same traffic, MSS applies only the first ACL match and ignores any other matches.

Examples — The following command maps security ACL *acl_133* to port 4 for incoming packets:

```
WX4400 set security acl map acl_133 port 4 in
success: change accepted.
```

See Also

- **clear security acl map** on page 539
- **commit security acl** on page 541
- **set mac-user attr** on page 261
- **set mac-usergroup attr** on page 267
- **set security acl** on page 552
- **set user attr** on page 273
- **set usergroup** on page 275
- **display security acl map** on page 546

**set security acl
hit-sample-rate**

Specifies the time interval, in seconds, at which the packet counter for each security ACL is sampled for display. The counter counts the number of packets filtered by the security ACL — or “hits.”

Syntax — `set security acl hit-sample-rate seconds`

- *seconds* — Number of seconds between samples. A sample rate of 0 (zero) disables the sample process.

Defaults — By default, the hits are not sampled.

Access — Enabled.

History — Introduced in MSS Version 3.0. Syntax changed from **hit-sample-rate *seconds*** to **set security acl hit-sample-rate *seconds***, to allow the command to be saved in the configuration file.

Usage — To view counter results for a particular ACL, use the **display security acl info *acl-name*** command. To view the hits for all security ACLs, use the **display security acl hits** command.

Examples — The first command sets MSS to sample ACL hits every 15 seconds. The second and third commands display the results. The results show that 916 packets matching *security acl_153* were sent since the ACL was mapped.

```
WX4400# set security acl hit-sample-rate 15
WX4400# display security acl info acl_153
ACL information for acl_153
set security acl ip acl_153 (hits #3 916)
-----
1. permit IP source IP 20.1.1.1 0.0.0.0 destination IP any enable-hits
WX4400# display security acl hits
ACL hit counters
Index Counter          ACL-name
-----
      1              0 acl_2
      2              0 acl_175
      3             916 acl_153
```

See Also

- **display security acl hits** on page 544
- **display security acl info** on page 545

15

CRYPTOGRAPHY COMMANDS

A digital certificate is a form of electronic identification for computers. The WX requires digital certificates to authenticate its communications to 3WXM and Web Manager, to WebAAA clients, and to Extensible Authentication Protocol (EAP) clients for which the WX performs all EAP processing. Certificates can be generated on the WX or obtained from a certificate authority (CA). Keys contained within the certificates allow the WX, its servers, and its wireless clients to exchange information secured by encryption.



If the switch does not already have certificates, MSS automatically generates the missing ones the first time you boot using MSS Version 4.2 or later. You do not need to install certificates unless you want to replace the ones automatically generated by MSS. (For more information, see the “Certificates Automatically Generated by MSS” section in the “Managing Keys and Certificates” chapter of the [Wireless LAN Switch and Controller Configuration Guide](#).)



Before installing a new certificate, verify with the `display timedate` and `display timezone` commands that the WX is set to the correct date, time, and time zone. Otherwise, certificates might not be installed correctly.

Commands by Usage

This chapter presents cryptography commands alphabetically. Use Table 88 to locate commands in this chapter based on their use.

Table 88 Cryptography Commands by Usage

Type	Command
Encryption Keys	crypto generate key on page 565
	display crypto key ssh on page 576
	display crypto key domain on page 576
PKCS #7 Certificates	crypto generate request on page 566
	crypto ca-certificate on page 562
	display crypto ca-certificate on page 573
	crypto certificate on page 564
PKCS #12 Certificate	display crypto certificate on page 574
	crypto otp on page 570
Self-Signed Certificate	crypto pkcs12 on page 572
	crypto generate self-signed on page 568

crypto ca-certificate

Installs a certificate authority's own PKCS #7 certificate into the WX certificate and key storage area.

Syntax — **crypto ca-certificate** {**admin** | **eap** | **web**}

PEM-formatted certificate

- **admin** — Stores the certificate authority's certificate that signed the administrative certificate for the WX switch.
The administrative certificate authenticates the WX to 3Com wireless switch manager (3XWM) or Web View.
- **eap** — Stores the certificate authority's certificate that signed the Extensible Authentication Protocol (EAP) certificate for the WX switch.
The EAP certificate authenticates the WX to 802.1X supplicants (clients).
- **web** — Stores the certificate authority's certificate that signed the WebAAA certificate for the WX switch.
The Web certificate authenticates the WX to clients who use WebAAA.

- *PEM-formatted certificate* — ASCII text representation of the certificate authority PKCS #7 certificate, consisting of up to 5120 characters that you have obtained from the certificate authority.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

Usage — The Privacy-Enhanced Mail protocol (PEM) format is used for representing a PKCS #7 certificate in ASCII text. PEM uses base64 encoding to convert the certificate to ASCII text, then puts the encoded text between the following delimiters:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

To use this command, you must already have obtained a copy of the certificate authority's certificate as a PKCS #7 object file. Then do the following:

- 1 Open the PKCS #7 object file with an ASCII text editor such as Notepad or vi.
- 2 Enter the **crypto ca-certificate** command on the CLI command line.
- 3 When MSS prompts you for the PEM-formatted certificate, paste the PKCS #7 object file onto the command line.

Examples — The following command adds the certificate authority's certificate to WX certificate and key storage:

```
WX4400# crypto ca-certificate admin
Enter PEM-encoded certificate
-----BEGIN CERTIFICATE-----
MIIDwDCCA2qgAwIBAgIQL2jvuu4P05FAQCyewU3oJANBgkqhkiG9wOBAQUFADCB
mzerMClaweVQQTToewi\wpoer0QWNFNk90044mbdr11277SWQ8G7DiwYUtrqoQplKJvxz
.....
Lm8wmVYxP56M;CUAm908C2foYgOY40=
-----END CERTIFICATE-----
```

See Also

- **display crypto ca-certificate** on page 573

crypto certificate

Installs one of the WX switch's PKCS #7 certificates into the certificate and key storage area on the WX switch. The certificate, which is issued and signed by a certificate authority, authenticates the WX switch either to 3WXM or Web Manager, or to 802.1X supplicants (clients).

Syntax — **crypto certificate** {**admin** | **eap** | **web**}

PEM-formatted certificate

- **admin** — Stores the certificate authority's administrative certificate, which authenticates the WX switch to 3WXM or Web Manager.
- **eap** — Stores the certificate authority's Extensible Authentication Protocol (EAP) certificate, which authenticates the WX switch to 802.1X supplicants (clients).
- **web** — Stores the certificate authority's WebAAA certificate, which authenticates the WX to clients who use WebAAA.
- *PEM-formatted certificate* — ASCII text representation of the PKCS #7 certificate, consisting of up to 5120 characters, that you have obtained from the certificate authority.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

Usage — To use this command, you must already have generated a certificate request with the **crypto generate request** command, sent the request to the certificate authority, and obtained a signed copy of the WX switch certificate as a PKCS #7 object file. Then do the following:

- 1 Open the PKCS #7 object file with an ASCII text editor such as Notepad or vi.
- 2 Enter the **crypto certificate** command on the CLI command line.
- 3 When MSS prompts you for the PEM-formatted certificate, paste the PKCS #7 object file onto the command line.

The WX switch verifies the validity of the public key associated with this certificate before installing it, to prevent a mismatch between the WX switch's private key and the public key in the installed certificate.

Examples — The following command installs a certificate:

```
WX4400# crypto certificate admin
Enter PEM-encoded certificate
-----BEGIN CERTIFICATE-----
MIIBdTCP3wIBADA2MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQOEExGjAYBgNVBAMU
EXRlY2hwdWJzQHRycHouY29tMIGfMAOGCSqGSIb3DQEBAQAA4GNADCBiQKBgQC4
.....
2L8Q9tk+G2As84QYLm8wmVY>xP56M;CUAm908C2foYgOY40=
-----END CERTIFICATE-----
```

See Also

- **crypto generate request** on page 566
- **crypto generate self-signed** on page 568

crypto generate key Generates an RSA public-private encryption key pair that is required for a Certificate Signing Request (CSR) or a self-signed certificate. For SSH, the command generates an SSH authentication key.

Syntax — `crypto generate key {admin | domain | eap | ssh | web} {128 | 512 | 1024 | 2048}`

- **admin** — Generates an administrative key pair for authenticating the WX switch to 3WXM or Web Manager.
- **domain** — Generates a key pair for securing the management traffic between WX switches.
- **eap** — Generates an EAP key pair for authenticating the WX switch to 802.1X supplicants (clients).
- **ssh** — Generates a key pair for authenticating the WX switch to Secure Shell (SSH) clients.
- **web** — Generates an administrative key pair for authenticating the WX switch to WebAAA clients.
- **128 | 512 | 1024 | 2048** — Length of the key pair in bits.
The minimum key size for SSH is 1024.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

Usage — You can overwrite a key by generating another key of the same type.

SSH requires an SSH authentication key, but you can allow MSS to generate it automatically. The first time an SSH client attempts to access the SSH server on a WX switch, the switch automatically generates a 1024-byte SSH key. If you want to use a 2048-byte key instead, use the **crypto generate key ssh 2048** command to generate one.

Examples — To generate an administrative key for use with 3WXM, type the following command:

```
WX4400# crypto generate key admin 1024
key pair generated
```

See Also

- **display crypto key ssh** on page 576

crypto generate request

Generates a Certificate Signing Request (CSR). This command outputs a PEM-formatted PKCS #10 text string that you can cut and paste to another location for delivery to a certificate authority.

This command generates either an administrative CSR for use with 3WXM and Web View, or an EAP CSR for use with 802.1X clients.

Syntax — **crypto generate request** {**admin** | **eap** | **web**}

- **admin** — Generates a request for an administrative certificate to authenticate the WX switch to 3WXM or Web Manager.
- **eap** — Generates a request for an EAP certificate to authenticate the WX switch to 802.1X supplicants (clients).
- **web** — Generates a request for a WebAAA certificate to authenticate the WX switch to WebAAA clients.

After you type the command, you are prompted for the following variables:

- **Country Name** *string* — (Optional) Specify the abbreviation for the country in which the WX switch is operating, in 2 alphanumeric characters with no spaces.

- **State Name** *string* — (Optional) Specify the name of the state, in up to 64 alphanumeric characters. Spaces are allowed.
- **Locality Name** *string* — (Optional) Specify the name of the locality, in up to 80 alphanumeric characters with no spaces.
- **Organizational Name** *string* — (Optional) Specify the name of the organization, in up to 80 alphanumeric characters with no spaces.
- **Organizational Unit** *string* — (Optional) Specify the name of the organizational unit, in up to 80 alphanumeric characters with no spaces.
- **Common Name** *string* — Specify a unique name for the WX switch, in up to 80 alphanumeric characters with no spaces. Use a fully qualified name if such names are supported on your network. This field is required.
- **Email Address** *string* — (Optional) Specify your email address, in up to 80 alphanumeric characters with no spaces.
- **Unstructured Name** *string* — (Optional) Specify any name, in up to 80 alphanumeric characters with no spaces.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1. Maximum string length for State Name increased from two to 64 alphanumeric characters.

Usage — To use this command, you must already have generated a public-private encryption key pair with the **crypto generate key** command.

Enter **crypto generate request admin**, **crypto generate request eap**, or **crypto generate request web** and press Enter. When you are prompted, type the identifying values in the fields, or press Enter if the field is optional. You must enter a common name for the WX switch.

This command outputs a PKCS #10 text string in Privacy-Enhanced Mail protocol (PEM) format that you paste to another location for submission to the certificate authority. You then send the request to the certificate authority to obtain a signed copy of the WX switch certificate as a PKCS #7 object file.

After you type the command, you are prompted for the following variables:

- **Country Name** *string* — (Optional) Specify the abbreviation for the country in which the WX switch is operating, in 2 alphanumeric characters with no spaces.
- **State Name** *string* — (Optional) Specify the abbreviation for the name of the state, in 2 alphanumeric characters with no spaces.
- **Locality Name** *string* — (Optional) Specify the name of the locality, in up to 80 alphanumeric characters with no spaces.
- **Organizational Name** *string* — (Optional) Specify the name of the organization, in up to 80 alphanumeric characters with no spaces.
- **Organizational Unit** *string* — (Optional) Specify the name of the organizational unit, in up to 80 alphanumeric characters with no spaces.
- **Common Name** *string* — Specify a unique name for the WX switch, in up to 80 alphanumeric characters with no spaces. Use a fully qualified name if such names are supported on your network. This field is required.

Note: If you are generating a WebAAA (web) certificate, use a common name that looks like a domain name (two or more strings connected by dots, with no spaces). For example, use `common.name` instead of `common name`. The string is not required to be an actual domain name. It simply needs to be formatted like one.

- **Email Address** *string* — (Optional) Specify your email address, in up to 80 alphanumeric characters with no spaces.
- **Unstructured Name** *string* — (Optional) Specify any name, in up to 80 alphanumeric characters with no spaces.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

Usage — To use this command, you must already have generated a public-private encryption key pair with the **crypto generate key** command.

To generate a self-signed administrative certificate, type the following command:

```
WX4400# crypto generate self-signed admin
Country Name:
State Name:
Locality Name:
Organizational Name:
Organizational Unit:
Common Name: wx1@example.com
Email Address:
Unstructured Name:
success: self-signed cert for admin generated
```

See Also

- **crypto certificate** on page 564
- **crypto generate key** on page 565

crypto otp

Sets a one-time password (OTP) for use with the **crypto pkcs12** command.

Syntax — **crypto otp** {**admin** | **eap** | **web**} *one-time-password*

- **admin** — Creates a one-time password for installing a PKCS #12 object file for an administrative certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the WX switch to 3WXM or Web Manager.
- **eap** — Creates a one-time password for installing a PKCS #12 object file for an EAP certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the WX switch to 802.1X supplicants (clients).
- **web** — Creates a one-time password for installing a PKCS #12 object file for a WebAAA certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the WX switch to WebAAA clients.
- *one-time-password* — Password of at least 1 alphanumeric character, with no spaces, for clients other than Microsoft Windows clients. The password must be the same as the password protecting the PKCS #12 object file.

Note: On an WX switch that handles communications to and from Microsoft Windows clients, use a one-time password of 31 characters or fewer.

The following characters *cannot* be used as part of the one-time password of a PKCS #12 file:

- Quotation marks (" ")
- Question mark (?)
- Ampersand (&)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

Usage — The password allows the public-private key pair and certificate to be installed together from the same PKCS #12 object file. MSS erases the one-time password after processing the **crypto pkcs12** command or when you reboot the WX switch.

3Com recommends that you create a password that is memorable to you but is not subject to easy guesses or a dictionary attack. For best results, create a password of alphanumeric uppercase and lowercase characters.

Examples — The following command creates the one-time password *hap9iN#ss* for installing an EAP certificate and key pair:

```
WX4400# crypto generate otp eap hap9iN#ss  
OTP set
```

See Also

- **crypto pkcs12** on page 572

crypto pkcs12

Unpacks a PKCS #12 object file into the certificate and key storage area on the WX switch. This object file contains a public-private key pair, an WX certificate signed by a certificate authority, and the certificate authority's certificate.

Syntax — `crypto pkcs12 {admin | eap | web} file-location-url`

- **admin** — Unpacks a PKCS #12 object file for an administrative certificate and key pair — and optionally the certificate authority's own certificate — for authenticating the WX switch to 3WXM or Web Manager.
- **eap** — Unpacks a PKCS #12 object file for an EAP certificate and key pair — and optionally the certificate authority's own certificate — for authenticating the WX switch to 802.1X supplicants (clients).
- **web** — Unpacks a PKCS #12 object file for a WebAAA certificate and key pair — and optionally the certificate authority's own certificate — for authenticating the WX switch to WebAAA clients.
- *file-location-url* — Location of the PKCS #12 object file to be installed. Specify a location of between 1 and 128 alphanumeric characters, with no spaces.

Defaults — The password you enter with the **crypto otp** command must be the same as the one protecting the PKCS #12 file.

Access — Enabled.

History — Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

Usage — To use this command, you must have already created a one-time password with the **crypto otp** command.

You must also have the PKCS #12 object file available. You can download a PKCS #12 object file via TFTP from a remote location to the local nonvolatile storage system on the WX switch.

Examples — The following commands copy a PKCS #12 object file for an EAP certificate and key pair—and optionally the certificate authority's own certificate—from a TFTP server to nonvolatile storage on the WX switch, create the one-time password *hap9iN#ss*, and unpack the PKCS #12 file:

```
WX4400# copy tftp://192.168.253.1/2048full.p12 2048full.p12
success: received 637 bytes in 0.253 seconds [ 2517
bytes/sec]
WX4400# crypto otp eap hap9iN#ss
OTP set
WX4400# crypto pkcs12 eap 2048full.p12
Unwrapped from PKCS12 file:
    keypair
    device certificate
    CA certificate
```

See Also

- **crypto otp** on page 570

display crypto ca-certificate

Displays information about the certificate authority's PEM-encoded PKCS #7 certificate.

Syntax — `display crypto ca-certificate {admin | eap | web}`

- **admin** — Displays information about the certificate authority's certificate that signed the administrative certificate for the WX switch. The administrative certificate authenticates the WX to 3WXM or Web View.
- **eap** — Displays information about the certificate authority's certificate that signed the Extensible Authentication Protocol (EAP) certificate for the WX switch. The EAP certificate authenticates the WX switch to 802.1X supplicants (clients).
- **web** — Displays information about the certificate authority's certificate that signed the WebAAA certificate for the WX switch. The WebAAA certificate authenticates the WX switch to WebAAA clients.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

Examples — To display information about the certificate of a certificate authority, type the following command:

```
WX4400# display crypto ca-certificate
```

Table 89 describes the fields in the display.

Table 89 display crypto ca-certificate Output

Fields	Description
Version	Version of the X.509 certificate.
Serial Number	A unique identifier for the certificate or signature.
Subject	Name of the certificate owner.
Signature Algorithm	Algorithm that created the signature, such as RSA MD5 or RSA SHA.
Issuer	Certificate authority that issued the certificate or signature.
Validity	Time period for which the certificate is valid.

See Also

- **crypto ca-certificate** on page 562
- **display crypto certificate** on page 574

display crypto certificate

Displays information about one of the cryptographic certificates installed on the WX switch.

Syntax — `display crypto certificate {admin | eap | web}`

- **admin** — Displays information about the administrative certificate that authenticates the WX switch to 3WXM or Web Manager.
- **eap** — Displays information about the EAP certificate that authenticates the WX switch to 802.1X supplicants (clients).
- **web** — Displays information about the WebAAA certificate that authenticates the WX switch to WebAAA clients.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

Usage — You must have generated a self-signed certificate or obtained a certificate from a certificate authority before displaying information about the certificate.

Examples — To display information about a cryptographic certificate, type the following command:

```
WX4400# display crypto certificate eap
```

Table 90 describes the fields of the display.

Table 90 crypto certificate Output

Fields	Description
Version	Version of the X.509 certificate.
Serial Number	A unique identifier for the certificate or signature.
Subject	Name of the certificate owner.
Signature Algorithm	Algorithm that created the signature, such as RSA MD5 or RSA SHA.
Issuer	Certificate authority that issued the certificate or signature.
Validity	Time period for which the certificate is valid.

See Also [crypto generate key](#) on page 565

display crypto key domain

Displays domain key information.

Syntax — `display crypto key domain`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To display domain key information, type the following command:

```
WX4400# display crypto key domain
```

See Also `crypto generate key` on page 565

display crypto key ssh

Displays SSH authentication key information. This command displays the checksum (also called a *fingerprint*) of the public SSH authentication key. When you connect to the WX switch with an SSH client, you can compare the SSH key checksum displayed by the WX switch with the one displayed by the client to verify that you really are connected to the WX switch and not another device. Generally, SSH clients remember the encryption key after the first connection, so you need to check the key only once.

Syntax — `display crypto key ssh`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To display SSH key information, type the following command:

```
WX4400# display crypto key ssh
ec:6f:56:7f:d1:fd:c0:28:93:ae:a4:f9:7c:f5:13:04
```

See Also `crypto generate key` on page 565

16

RADIUS AND SERVER GROUP COMMANDS

Use RADIUS commands to set up communication between a WX switch and groups of up to four RADIUS servers for remote authentication, authorization, and accounting (AAA) of administrators and network users.

Commands by Usage

This chapter presents RADIUS commands alphabetically. Use Table 91 to locate commands in this chapter based on their uses.

Table 91 RADIUS Commands by Usage

Type	Command
RADIUS Client	set radius client system-ip on page 584
	clear radius client system-ip on page 579
RADIUS Servers	set radius on page 582
	set radius server on page 587
	clear radius on page 578
	clear radius server on page 581
Server Groups	set server group on page 589
	set server group load-balance on page 590
	clear server group on page 581
RADIUS Proxy	set radius proxy client on page 585
	set radius proxy port on page 586
	clear radius proxy client on page 580
	clear radius proxy port on page 580

(For information about RADIUS attributes, see the RADIUS appendix in the [Wireless LAN Switch and Controller Configuration Guide](#).)

clear radius

Resets parameters that were globally configured for RADIUS servers to their default values.

Syntax — `clear radius {deadtime | key | retransmit | timeout }`

- **deadtime** — Number of minutes to wait after declaring an unresponsive RADIUS server unavailable before retrying the RADIUS server.
- **key** — Password (shared secret key) used to authenticate to the RADIUS server.
- **retransmit** — Number of transmission attempts made before declaring an unresponsive RADIUS server unavailable.
- **timeout** — Number of seconds to wait for the RADIUS server to respond before retransmitting.

Defaults — Global RADIUS parameters have the following default values:

- **deadtime**—0 (zero) minutes (The WX switch does not designate unresponsive RADIUS servers as unavailable.)
- **key**—No key
- **retransmit**—3 (the total number of attempts, including the first attempt)
- **timeout**—5 seconds

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — To override the globally set values on a particular RADIUS server, use the **set radius server** command.

Examples — To reset all global RADIUS parameters to their factory defaults, type the following commands:

```
WX4400# clear radius deadtime
success: change accepted.
WX4400# clear radius key
success: change accepted.
WX4400# clear radius retransmit
success: change accepted.
```

```
WX4400# clear radius timeout
success: change accepted.
```

See Also

- **display aaa** on page 229
- **set radius** on page 582
- **set radius server** on page 587

clear radius client system-ip

Removes the WX switch's system IP address from use as the permanent source address in RADIUS client requests from the switch to its RADIUS server(s).

Syntax — `clear radius client system-ip`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The **clear radius client system-ip** command causes the WX switch to use the IP address of the interface through which it sends a RADIUS client request as the source IP address. The WX switch selects a source interface address based on information in its routing table as the source address for RADIUS packets leaving the switch.

Examples — To clear the system IP address as the permanent source address for RADIUS client requests, type the following command:

```
WX4400# clear radius client system-ip
success: change accepted.
```

See Also

- **display aaa** on page 229
- **set radius client system-ip** on page 584

clear radius proxy client

Removes RADIUS proxy client entries for third-party APs.

Syntax — `clear radius proxy client all`

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.0.

Examples — The following command clears all RADIUS proxy client entries from the switch:

```
WX4400# clear radius proxy client all
success: change accepted.
```

See Also

- **set radius proxy client** on page 585

clear radius proxy port

Removes RADIUS proxy ports configured for third-party APs.

Syntax — `clear radius proxy port all`

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.0.

Examples — The following command clears all RADIUS proxy port entries from the switch:

```
WX4400# clear radius proxy port all
success: change accepted.
```

See Also

- **set radius proxy port** on page 586

clear radius server Removes the named RADIUS server from the WX configuration.

Syntax — `clear radius server server-name`

- *server-name* — Name of a RADIUS server configured to perform remote AAA services for the WX switch.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes the RADIUS server *rs42* from a list of remote AAA servers:

```
WX4400# clear radius server rs42
success: change accepted.
```

See Also

- **display aaa** on page 229
- **set radius server** on page 587

clear server group Removes a RADIUS server group from the configuration, or disables load balancing for the group.

Syntax — `clear server group group-name [load-balance]`

- *group-name* — Name of a RADIUS server group configured to perform remote AAA services for WX switches.
- **load-balance** — Ability of group members to share demand for services among servers.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Deleting a server group removes the server group from the configuration. However, the members of the server group remain.

Examples — To remove the server group *sg-77* type the following command:

```
WX4400# clear server group sg-77
success: change accepted.
```

To disable load balancing in a server group *shorebirds*, type the following command:

```
WX4400# set server group shorebirds load-balance disable
success: change accepted.
```

See Also

- **set server group** on page 589

set radius

Configures global defaults for RADIUS servers that do not explicitly set these values themselves. By default, the WX switch automatically sets all these values except the password (key).

Syntax — `set radius {deadtime minutes | encrypted-key string | key string | retransmit number | timeout seconds}`

- **deadtime *minutes*** — Number of minutes the WX switch waits after declaring an unresponsive RADIUS server unavailable before retrying the RADIUS server. You can specify from 0 to 1440 minutes.
- **encrypted keyword *string*** — Password (shared secret key) used to authenticate to the RADIUS server, entered in its encrypted form. You must provide the same encrypted password that is defined on the RADIUS server. The password can be 1 to 64 characters long, with no spaces or tabs.

MSS does not encrypt the string you enter, and instead displays the string in **display config** and **display aaa** output exactly as you entered it.

Note: Use this option only if you are entering the key in its encrypted form. To enter the key in unencrypted form, use the **key *string*** option instead.

- **key *string*** — Password (shared secret key) used to authenticate to the RADIUS server. You must provide the same password that is defined on the RADIUS server. The password can be 1 to 64 characters long, with no spaces or tabs.

MSS encrypts the display form of the string in **display config** and **display aaa** output.

- **retransmit** *number* — Number of transmission attempts the WX switch makes before declaring an unresponsive RADIUS server unavailable. You can specify from 1 to 100 retries.
- **timeout** *seconds* — Number of seconds the WX switch waits for the RADIUS server to respond before retransmitting. You can specify from 1 to 65,535.

Defaults — Global RADIUS parameters have the following default values:

- **deadtime** — 0 (zero) minutes (The WX switch does not designate unresponsive RADIUS servers as unavailable.)
- **encrypted-key**—No key
- **key** — No key
- **retransmit** — 3 (the total number of attempts, including the first attempt)
- **timeout** — 5 seconds

Access — Enabled.

History —Introduced in MSS Version 3.0. The **encrypted-key** option was added in Version 4.2.

Usage — You can specify only one parameter per command line.

Examples — The following commands sets the dead time to 5 minutes, the RADIUS key to *goody*, the number of retransmissions to 1, and the timeout to 21 seconds on all RADIUS servers connected to the WX switch:

```
WX1200# set radius deadtime 5
success: change accepted.
WX1200# set radius key goody
success: change accepted.
WX1200# set radius retransmit 1
success: change accepted.
WX1200# set radius timeout 21
success: change accepted.
```

See Also

- **clear radius server** on page 581
- **display aaa** on page 229
- **set radius server** on page 587

set radius client system-ip

Causes all RADIUS requests to be sourced from the IP address specified by the **set system ip-address** command, providing a permanent source IP address for RADIUS packets sent from the WX switch.

Syntax — `set radius client system-ip`

Defaults — None. If you do not use this command, RADIUS packets leaving the WX have the source IP address of the outbound interface, which can change as routing conditions change.

Examples — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The WX system IP address must be set before you use this command.

Examples — The following command sets the WX system IP address as the address of the RADIUS client:

```
WX4400# set radius client system-ip
success: change accepted.
```

See Also

- **clear radius client system-ip** on page 579
- **set system idle-timeout** on page 65

set radius proxy client

Adds a RADIUS proxy entry for a third-party AP. The proxy entry specifies the IP address of the AP and the UDP ports on which the WX switch listens for RADIUS traffic from the AP.

Syntax — `set radius proxy client address ip-address [acct-port acct-udp-port-number] [port udp-port-number] key string`

- **address** *ip-address* — IP address of the third-party AP. Enter the address in dotted decimal notation.
- **port** *udp-port-number* — UDP port on which the WX switch listens for RADIUS access-requests from the AP.
- **acct-port** *acct-udp-port-number* — UDP port on which the WX switch listens for RADIUS stop-accounting records from the AP.
- **key** *string* — Password (shared secret key) the WX switch uses to authenticate and encrypt RADIUS communication.

Defaults — The default UDP port number for access-requests is 1812. The default UDP port number for stop-accounting records is 1813.

Access — Enabled.

History — Introduced in MSS 4.0.

Usage — AAA for third-party AP users has additional configuration requirements. See the “Configuring AAA for Users of Third-Party APs” section in the “Configuring AAA for Network Users” chapter of the *Wireless LAN Switch and Controller Configuration Guide*.

Examples — The following command configures a RADIUS proxy entry for a third-party AP RADIUS client at 10.20.20.9, sending RADIUS traffic to the default UDP ports 1812 and 1813 on the WX:

```
WX4400# set radius proxy client address 10.20.20.9 key radkey1
success: change accepted.
```

See Also

- **clear radius proxy client** on page 580
- **set authentication proxy** on page 253
- **set radius proxy port** on page 586

set radius proxy port

Configures the WX port connected to a third-party AP as a RADIUS proxy for the SSID supported by the AP.

Syntax — `set radius proxy port port-list [tag tag-value] ssid ssid-name`

- **port** *port-list* — WX port(s) connected to the third-party AP.
- **tag** *tag-value* — 802.1Q tag value in packets sent by the third-party AP for the SSID.
- **ssid** *ssid-name* — SSID supported by the third-party AP.

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.0.

Usage — AAA for third-party AP users has additional configuration requirements. See the “Configuring AAA for Users of Third-Party APs” section in the “Configuring AAA for Network Users” chapter of the [Wireless LAN Switch and Controller Configuration Guide](#).

Enter a separate command for each SSID, and its tag value, you want the WX to support.

Examples — The following command maps SSID *mycorp* to packets received on port 3 or 4, using 802.1Q tag value 104:

```
WX4400# set radius proxy port 3-4 tag 104 ssid mycorp
success: change accepted.
```

See Also

- **clear radius proxy port** on page 580
- **set authentication proxy** on page 253
- **set radius proxy client** on page 585

set radius server

Configures RADIUS servers and their parameters. By default, the WX switch automatically sets all these values except the password (key).

Syntax — **set radius server** *server-name*
[**address** *ip-address*] [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *number*] [**deadtime** *minutes*] [**key** *string*] [**encrypted-key** *string*] [**author-password** *password*]

- **server-name** — Unique name for this RADIUS server. Enter an alphanumeric string of up to 32 characters, with no blanks.
- **address** *ip-address* — IP address of the RADIUS server. Enter the address in dotted decimal notation.
- **auth-port** *port-number* — UDP port that the WX switch uses for authentication and authorization.
- **acct-port** *port-number* — UDP port that the WX switch uses for accounting.
- **timeout** *seconds* — Number of seconds the WX switch waits for the RADIUS server to respond before retransmitting. You can specify from 1 to 65,535 seconds.
- **retransmit** *number* — Number of transmission attempts made before declaring an unresponsive RADIUS server unavailable. You can specify from 1 to 100 retries.
- **deadtime** *minutes* — Number of minutes the WX switch waits after declaring an unresponsive RADIUS server unavailable before retrying that RADIUS server. Specify between 0 (zero) and 1440 minutes (24 hours). A zero value causes the switch to identify unresponsive servers as available.
- **key** *string* — Password (shared secret key) the WX switch uses to authenticate to the RADIUS server. You must provide the same password that is defined on the RADIUS server. The password can be 1 to 64 characters long, with no spaces or tabs.
 - Use the **key** option to enter the string in its unencrypted form. MSS encrypts the displayed form of the string in **display config** and **display aaa** output.
 - To enter the string in its encrypted form instead, use the **encrypted-key** option. MSS does not encrypt the string you enter, and instead displays the string exactly as you enter it.

- **author-password** *password* — Password used for authorization to a RADIUS server for MAC users. Specify a password of up to 64 alphanumeric characters with no spaces or tabs.

Defaults — Default values are listed below:

- **auth-port** — UDP port 1812
- **acct-port** — UDP port 1813
- **timeout** — 5 seconds
- **retransmit** — 3 (the total number of attempts, including the first attempt)
- **deadtime** — 0 (zero) minutes (The WX switch does not designate unresponsive RADIUS servers as unavailable.)
- **key** — No key
- **encrypted-key** — No key
- **author-password** — When using RADIUS for authentication, a MAC user's MAC address is also used as the default authorization password for that user, and no global authorization password is set. A last-resort user's default authorization password is *3Com*.

Access — Enabled.

History — Introduced in MSS Version 3.0. The **encrypted-key** option was added in Version 4.2.

Usage — For a given RADIUS server, the first instance of this command must set both the server name and the IP address and can include any or all of the other optional parameters. Subsequent instances of this command can be used to set optional parameters for a given RADIUS server.

To configure the server as a remote authenticator for the WX switch, you must add it to a server group with the **set server group** command.

Do not use the same name for a RADIUS server and a RADIUS server group.

Examples — To set a RADIUS server named RS42 with IP address 198.162.1.1 to use the default accounting and authorization ports with a timeout interval of 30 seconds, two transmit attempts, 5 minutes of dead time, and a key string of *keys4u*, type the following command:

```
WX1200# set radius server RS42 address 198.162.1.1 timeout 30
retransmit 2 deadtime 5 key keys4U
```

See Also

- **display aaa** on page 229
- **set authentication admin** on page 239
- **set authentication console** on page 241
- **set authentication dot1x** on page 243
- **set authentication mac** on page 247
- **set authentication mac** on page 247
- **set authentication web** on page 254
- **set radius** on page 582
- **set server group** on page 589

set server group

Configures a group of one to four RADIUS servers.

Syntax — **set server group** *group-name* **members** *server-name1* [*server-name2*] [*server-name3*] [*server-name4*]

- *group-name* — Server group name of up to 32 characters, with no spaces or tabs.
- **members** *server-name1*, *server-name2*, *server-name3*, *server-name4* — The names of one or more configured RADIUS servers. You can enter up to four server names.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must assign all group members simultaneously, as shown in the example. To enable load balancing, use **set server group load-balance enable**.

Do not use the same name for a RADIUS server and a RADIUS server group.

Examples — To set server group *shorebirds* with members *heron*, *egret*, and *sandpiper*, type the following command:

```
WX1200# set server group shorebirds members heron egret
sandpiper
success: change accepted.
```

See Also

- **clear server group** on page 581
- **display aaa** on page 229
- **set server group load-balance** on page 590

set server group load-balance

Enables or disables load balancing among the RADIUS servers in a server group.

Syntax — `set server group group-name load-balance {enable | disable}`

- *group-name* — Server group name of up to 32 characters.
- **load-balance enable | disable** — Enables or disables load balancing of authentication requests among the servers in the group.

Defaults — Load balancing is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You can optionally enable load balancing after assigning the server group members. If you configure load balancing, MSS sends each AAA request to a separate server, starting with the first one on the list and skipping unresponsive servers. If no server in the group responds, MSS moves to the next method configured with **set authentication** and **set accounting**.

In contrast, if load balancing is *not* configured, MSS always begins with the first server in the list and sends unfulfilled requests to each subsequent server in the group before moving on to the next configured AAA method.

Examples — To enable load balancing between the members of server group *shorebirds*, type the following command:

```
WX1200# set server group shorebirds load-balance enable
success: change accepted.
```

To disable load balancing between *shorebirds* server group members, type the following command:

```
WX1200# set server group shorebirds load-balance disable
success: change accepted.
```

See Also

- **clear server group** on page 581
- **clear radius server** on page 581
- **display aaa** on page 229
- **set server group** on page 589

17

802.1X MANAGEMENT COMMANDS

Use 802.1X management commands to modify the default settings for IEEE 802.1X sessions on an WX. For best results, change the settings only if you are aware of a problem with 802.1X performance on the WX.



CAUTION: 802.1X parameter settings are global for all SSIDs configured on the switch.

Commands by Usage

This chapter presents 802.1X commands alphabetically. Use Table 92 to locate commands in this chapter based on their use. For information about configuring 802.1X commands for user authentication, see “AAA Commands” on page 211.

Table 92 802.1X Commands by Usage

Type	Command
Wired Authentication Port Control	set dot1x port-control on page 606
	clear dot1x port-control on page 595
	set dot1x authcontrol on page 602
Keys	set dot1x key-tx on page 604
	set dot1x tx-period on page 610
	clear dot1x tx-period on page 599
	set dot1x wep-rekey on page 611
Bonded Authentication	set dot1x wep-rekey-period on page 612
	clear dot1x bonded-period on page 594
Reauthentication	set dot1x bonded-period on page 603
	set dot1x reauth on page 607
Reauthentication, cont.	set dot1x reauth-max on page 608
	clear dot1x reauth-max on page 597

Table 92 802.1X Commands by Usage (continued)

Type	Command
	set dot1x reauth-period on page 609
	clear dot1x reauth-period on page 597
Retransmission	set dot1x max-req on page 605
	clear dot1x max-req on page 595
Quiet Period and Timeouts	set dot1x quiet-period on page 607
	clear dot1x quiet-period on page 596
	set dot1x timeout auth-server on page 609
	clear dot1x timeout auth-server on page 598
	set dot1x timeout supplicant on page 610
	clear dot1x timeout supplicant on page 598
Settings, Active Clients, and Statistics	display dot1x on page 599

clear dot1x bonded-period

Resets the Bonded Auth™ (bonded authentication) period to its default value. The bonded period is the number of seconds MSS retains session information for an authenticated machine while waiting for an 802.1X client on the machine to start (re)authentication for the user. When bonded authentication is enabled, it applies only to an 802.1X user whose authentication rule on the WX switch contains the **bonded** option.

Syntax — `clear dot1x bonded-period`

Defaults — The default bonded authentication period is 0 seconds, which disables the feature.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To reset the Bonded period to its default, type the following command:

```
WX4400# clear dot1x bonded-period
success: change accepted.
```

See Also

- **display dot1x** on page 599
- **set dot1x bonded-period** on page 603

clear dot1x max-req Resets to the default setting the number of Extensible Authentication Protocol (EAP) requests that the WX switch retransmits to a supplicant (client).

Syntax — `clear dot1x max-req`

Defaults — The default number is 20.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To reset the number of 802.1X requests the WX can send to the default setting, type the following command:

```
WX4400# clear dot1x max-req
success: change accepted.
```

See Also

- **display dot1x** on page 599
- **set dot1x max-req** on page 605

clear dot1x port-control Resets all wired authentication ports on the WX switch to default 802.1X authentication.

Syntax — `clear dot1x port-control`

By default, all wired authentication ports are set to **auto** and they process authentication requests as determined by the **set authentication dot1X** command.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command is overridden by the **set dot1x authcontrol** command. The **clear dot1x port-control** command returns port control to the method configured. This command applies only to wired authentication ports.

Examples — Type the following command to reset the wired authentication port control:

```
WX4400# clear dot1x port-control
success: change accepted.
```

See Also

- **display dot1x** on page 599
- **set dot1x port-control** on page 606

**clear dot1x
quiet-period**

Resets the quiet period after a failed authentication to the default setting.

Syntax — `clear dot1x quiet-period`

Defaults — The default is 60 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — Type the following command to reset the 802.1X quiet period to the default:

```
WX4400# clear dot1x quiet-period
success: change accepted.
```

See Also

- **display dot1x** on page 599
- **set dot1x quiet-period** on page 607

**clear dot1x
reauth-max**

Resets the maximum number of reauthorization attempts to the default setting.

Syntax — `clear dot1x reauth-max`

Defaults — The default is 2 attempts.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — Type the following command to reset the maximum number of reauthorization attempts to the default:

```
WX4400# clear dot1x reauth-max
success: change accepted.
```

See Also

- **display dot1x** on page 599
- **set dot1x reauth-max** on page 608

**clear dot1x
reauth-period**

Resets the time period that must elapse before a reauthentication attempt, to the default time period.

Syntax — `clear dot1x reauth-period`

Defaults — The default is 3600 seconds (1 hour).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — Type the following command to reset the default reauthentication time period:

```
WX4400# clear dot1x reauth-period
success: change accepted.
```

See Also

- **display dot1x** on page 599
- **set dot1x reauth-period** on page 609

**clear dot1x timeout
auth-server**

Resets to the default setting the number of seconds that must elapse before the WX times out a request to a RADIUS server.

Syntax — `clear dot1x timeout auth-server`

Defaults — The default is 30 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To reset the default timeout for requests to an authentication server, type the following command:

```
WX4400# clear dot1x timeout auth-server
success: change accepted.
```

See Also

- **display dot1x** on page 599
- **set dot1x timeout auth-server** on page 609

**clear dot1x timeout
supplicant**

Resets to the default setting the number of seconds that must elapse before the WX switch times out an authentication session with a supplicant (client).

Syntax — `clear dot1x timeout supplicant`

Defaults — The default for the authentication timeout sessions is 30 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — Type the following command to reset the timeout period for an authentication session:

```
WX4400# clear dot1x timeout supplicant
success: change accepted.
```

See Also

- **display dot1x** on page 599
- **set dot1x timeout supplicant** on page 610

clear dot1x tx-period

Resets to the default setting the number of seconds that must elapse before the WX switch retransmits an EAP over LAN (EAPoL) packet.

Syntax — `clear dot1x tx-period`

Defaults — The default is 5 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — Type the following command to reset the EAPoL retransmission time:

```
WX4400# clear dot1x tx-period
success: change accepted.
```

See Also

- **display dot1x** on page 599
- **set dot1x tx-period** on page 610

display dot1x

Displays 802.1X client information for statistics and configuration settings.

Syntax — `display dot1x {clients | stats | config}`

- **clients** — Displays information about active 802.1X clients, including client name, MAC address, and state.
- **stats** — Displays global 802.1X statistics associated with connecting and authenticating.
- **config** — Displays a summary of the current configuration.

Defaults — None.

Access — Enabled.

History —Introduced in MSS Version 3.0. Format of 802.1X authentication rule information in **display dot1x config** output changed in MSS Version 3.2. The rules are still listed at the top of the display, but more information is shown for each rule.

Examples — Type the following command to display the 802.1X clients:

```
WX4400# display dot1x clients
MAC Address                State                Vlan                Identity
-----
00:20:a6:48:01:1f          Connecting          (unknown)
00:05:3c:07:6d:7c          Authenticated      vlan-it             EXAMPLE\jose
00:05:5d:7e:94:83          Authenticated      vlan-eng            EXAMPLE\singh
00:02:2d:86:bd:38          Authenticated      vlan-eng            bard@xmples.com
00:05:5d:7e:97:b4          Authenticated      vlan-eng            EXAMPLE\havel
00:05:5d:7e:98:1a          Authenticated      vlan-eng            EXAMPLE\nash
00:0b:be:a9:dc:4e          Authenticated      vlan-pm             xalik@xmples.com
00:05:5d:7e:96:e3          Authenticated      vlan-eng            EXAMPLE\mishan
00:02:2d:6f:44:77          Authenticated      vlan-eng            EXAMPLE\ethan
00:05:5d:7e:94:89          Authenticated      vlan-eng            EXAMPLE\fmarshall
00:06:80:00:5c:02          Authenticated      vlan-eng            EXAMPLE\bmccarthy
00:02:2d:6a:de:f2          Authenticated      vlan-pm             neailey@xmples.com
00:02:2d:5e:5b:76          Authenticated      vlan-pm             EXAMPLE\tamara
00:02:2d:80:b6:e1          Authenticated      vlan-cs             dmc@xmples.com
00:30:65:16:8d:69          Authenticated      vlan-wep            MAC authenticated
00:02:2d:64:8e:1b          Authenticated      vlan-eng            EXAMPLE\wong
```

Type the following command to display the 802.1X configuration:

```
WX1200# display dot1x config

802.1X user policy
-----
'host/bob-laptop.mycorp.com' on ssid 'mycorp' doing PASSTHRU
'bob.mycorp.com' on ssid 'mycorp' doing PASSTHRU (bonded)
```



```

802.1X parameter          setting
-----
supplicant timeout        30
auth-server timeout       30
quiet period              5
transmit period           5
reauthentication period   3600
maximum requests          2
key transmission          enabled
reauthentication          enabled
authentication control    enabled
WEP rekey period          1800
WEP rekey                 enabled
Bonded period             60

```

```

port 5, authcontrol: auto, max-sessions: 16
port 6, authcontrol: auto, max-sessions: 1
port 7, authcontrol: auto, max-sessions: 1
port 8, authcontrol: auto, max-sessions: 1

```

Type the following command to display 802.1X statistics:

```

WX4400# display dot1x stats
      802.1X statistic          value
-----
Enters Connecting:             709
Logoffs While Connecting:     112
Enters Authenticating:        467
Success While Authenticating:  0
Timeouts While Authenticating: 52
Failures While Authenticating: 0
Reauths While Authenticating:  0
Starts While Authenticating:  31
Logoffs While Authenticating:  0
Starts While Authenticated:    85
Logoffs While Authenticated:   1
Bad Packets Received:          0

```

Table 93 explains the counters in the **display dot1x stats** output.

Table 93 display dot1x stats Output

Field	Description
Enters Connecting	Number of times that the WX switch state transitions to the CONNECTING state from any other state.
Logoffs While Connecting	Number of times that the WX switch state transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPoL-Logoff message.
Enters Authenticating	Number of times that the state wildcard transitions.
Success While Authenticating	Number of times the WX switch state transitions from AUTHENTICATING from AUTHENTICATED, as a result of an EAP-Response/Identity message being received from the supplicant (client).
Timeouts While Authenticating	Number of times that the WX switch state wildcard transitions from AUTHENTICATING to ABORTING.
Failures While Authenticating	Number of times that the WX switch state wildcard transitions from AUTHENTICATION to HELD.
Reauths While Authenticating	Number of times that the WX switch state wildcard transitions from AUTHENTICATING to ABORTING, as a result of a reauthentication request (reAuthenticate = TRUE).
Starts While Authenticating	Number of times that the WX switch state wildcard transitions from AUTHENTICATING to ABORTING, as a result of an EAPoL-Start message being received from the Supplicant (client).
Logoffs While Authenticating	Number of times that the WX switch state wildcard transitions from AUTHENTICATING to ABORTING, as a result of an EAPoL-logoff message being received from the Supplicant (client).
Bad Packets Received	Number of EAPoL packets received that have an invalid version or type.

set dot1x authcontrol

Provides a global override mechanism for 802.1X authentication configuration on wired authentication ports.

Syntax — `set dot1x authcontrol {enable | disable}`

- **enable** — Allows all wired authentication ports running 802.1X to use the authentication specified per port by the **set dot1X port-control** command.
- **disable** — Forces all wired authentication ports running 802.1X to unconditionally accept all 802.1X authentication attempts with an EAP Success message (ForceAuth).

Defaults — By default, authentication control for individual wired authentication is enabled.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — This command applies only to wired authentication ports.

Examples — To enable per-port 802.1X authentication on wired authentication ports, type the following command:

```
WX4400# set dot1x authcontrol enable
success: dot1x authcontrol enabled.
```

See Also

- **display dot1x** on page 599
- **set dot1x port-control** on page 606

set dot1x bonded-period

Changes the Bonded Auth™ (bonded authentication) period, which is the number of seconds MSS retains session information for an authenticated machine while waiting for the 802.1X client on the machine to start (re)authentication for the user.

You must set the bonded period to longer than 0 seconds to enable bonded authentication.

Syntax — `set dot1x bonded-period seconds`

- *seconds* — Number of seconds MSS retains session information for an authenticated machine while waiting for a client to (re)authenticate on the same machine. You can change the bonded authentication period to a value from 1 to 300 seconds.

Defaults — The default bonded period is 0 seconds, which disables the feature.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — Normally, the Bonded Auth period needs to be set only if the network has Bonded Auth clients that use dynamic WEP, or use WEP-40 or WEP-104 encryption with WPA or RSN. These clients can be affected by the 802.1X reauthentication parameter or the RADIUS Session-Timeout parameter.

3Com recommends that you try 60 seconds, and change the period to a longer value only if clients are unable to authenticate within 60 seconds.

The bonded authentication period applies only to 802.1X authentication rules that contain the **bonded** option.

Examples — To set the bonded authentication period to 60 seconds, type the following command:

```
WX4400# set dot1x bonded-period 60
success: change accepted.
```

See Also

- **display dot1x** on page 599
- **clear dot1x bonded-period** on page 594

set dot1x key-tx

Enables or disables the transmission of encryption key information to the supplicant (client) in EAP over LAN (EAPoL) key messages, after authentication is successful.

Syntax — `set dot1x key-tx {enable | disable}`

- **enable** — Enables transmission of encryption key information to clients.
- **disable** — Disables transmission of encryption key information to clients.

Defaults — Key transmission is enabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — Type the following command to enable key transmission:

```
WX4400# set dot1x key-tx enable
success: dot1x key transmission enabled.
```

See Also

- **display dot1x** on page 599

set dot1x max-req

Sets the maximum number of times the WX retransmits an EAP request to a supplicant (client) before ending the authentication session.

Syntax — `set dot1x max-req number-of-retransmissions`

- *number-of-retransmissions* — Specify a value between 0 and 10.

Defaults — The default number of EAP retransmissions is 2.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To support SSIDs that have both 802.1X and static WEP clients, MSS sends a maximum of two ID requests, even if this parameter is set to a higher value. Setting the parameter to a higher value does affect all other types of EAP messages.

Examples — Type the following command to set the maximum number of EAP request retransmissions to three attempts:

```
WX4400# set dot1x max-req 3
success: dot1x max request set to 3.
```

See Also

- **clear dot1x max-req** on page 595
- **display dot1x** on page 599

**set dot1x
port-control**

Determines the 802.1X authentication behavior on individual wired authentication ports or groups of ports.

Syntax — `set dot1x port-control`
`{forceauth | forceunauth | auto} port-list`

- **forceauth** — Forces the specified wired authentication port(s) to *unconditionally authorize* all 802.1X authentication attempts, with an EAP success message.
- **forceunauth** — Forces the specified wired authentication port(s) to *unconditionally reject* all 802.1X authentication attempts with an EAP failure message.
- **auto** — Allows the specified wired authentication ports to process 802.1X authentication normally as determined for the user by the **set authentication dot1X** command.
- *port-list* — One or more wired authentication ports for which to set 802.1X port control.

Defaults — By default, wired authentication ports are set to **auto**.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command affects only wired authentication ports.

Examples — The following command forces port 1 to unconditionally accept all 802.1X authentication attempts:

```
WX4400# set dot1x port-control forceauth 1
success: authcontrol for 1 is set to FORCE-AUTH.
```

See Also

- **display port status** on page 79
- **display dot1x** on page 599

set dot1x quiet-period

Sets the number of seconds a WX remains quiet and does not respond to a supplicant after a failed authentication.

Syntax — `set dot1x quiet-period seconds`

- `seconds` — Specify a value between 0 and 65,535.

Defaults — The default is 60 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — Type the following command to set the quiet period to 90 seconds:

```
WX4400# set dot1x quiet-period 90
success: dot1x quiet period set to 90.
```

See Also

- **clear dot1x quiet-period** on page 596
- **set dot1x wep-rekey-period** on page 612

set dot1x reauth

Determines whether the WX switch allows the reauthentication of supplicants (clients).

Syntax — `set dot1x reauth {enable | disable}`

- `enable` — Permits reauthentication.
- `disable` — Denies reauthentication.

Defaults — Reauthentication is enabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — Type the following command to enable reauthentication of supplicants (clients):

```
WX4400# set dot1x reauth enable
success: dot1x reauthentication enabled.
```

See Also

- **display dot1x** on page 599
- **set dot1x reauth-max** on page 608
- **set dot1x reauth-period** on page 609

**set dot1x
reauth-max**

Sets the number of reauthentication attempts that the WX switch makes before the supplicant (client) becomes unauthorized.

Syntax — `set dot1x reauth-max number-of-attempts`

- *number-of-attempts* — Specify a value between 1 and 10.

Defaults — The default number of reauthentication attempts is 2.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — If the number of reauthentications for a wired authentication client is greater than the maximum number of reauthentications allowed, MSS sends an EAP failure packet to the client and removes the client from the network. However, MSS does not remove a wireless client from the network under these circumstances.

Examples — Type the following command to set the number of authentication attempts to 8:

```
WX4400# set dot1x reauth-max 8
success: dot1x max reauth set to 8.
```

See Also

- **display dot1x** on page 599
- **clear dot1x reauth-max** on page 597

set dot1x reauth-period

Sets the number of seconds that must elapse before the WX switch attempts reauthentication.

Syntax — `set dot1x reauth-period seconds`

- *seconds* — Specify a value between 60 (1 minute) and 1,641,600 (19 days).

Defaults — The default is 3600 seconds (1 hour).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — Type the following command to set the number of seconds to 100 before reauthentication is attempted:

```
WX4400# set dot1x reauth-period 100
success: dot1x auth-server timeout set to 100.
```

See Also

- **display dot1x** on page 599
- **clear dot1x reauth-period** on page 597

set dot1x timeout auth-server

Sets the number of seconds that must elapse before the WX switch times out a request to a RADIUS authentication server.

Syntax — `set dot1x timeout auth-server seconds`

- *seconds* — Specify a value between 1 and 65,535.

Defaults — The default is 30 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — Type the following command to set the authentication server timeout to 60 seconds:

```
WX4400# set dot1x timeout auth-server 60
success: dot1x auth-server timeout set to 60.
```

See Also

- **display dot1x** on page 599
- **clear dot1x timeout auth-server** on page 598

set dot1x timeout supplicant

Sets the number of seconds that must elapse before the WX switch times out an authentication session with a supplicant (client).

Syntax — `set dot1x timeout supplicant seconds`

- *seconds* — Specify a value between 1 and 65,535.

Defaults — The default is 30 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — Type the following command to set the number of seconds for authentication session timeout to 300:

```
WX4400# set dot1x timeout supplicant 300
success: dot1x supplicant timeout set to 300.
```

See Also

- **display dot1x** on page 599
- **clear dot1x timeout auth-server** on page 598

set dot1x tx-period

Sets the number of seconds that must elapse before the WX switch retransmits an EAPoL packet.

Syntax — `set dot1x tx-period seconds`

- *seconds* — Specify a value between 1 and 65,535.

Defaults — The default is 5 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — Type the following command to set the number of seconds before the WX switch retransmits an EAPoL packet to 300:

```
WX4400# set dot1x tx-period 300
success: dot1x tx-period set to 300.
```

See Also

- **display dot1x** on page 599
- **clear dot1x tx-period** on page 599

set dot1x wep-rekey

Enables or disables Wired Equivalency Privacy (WEP) rekeying for broadcast and multicast encryption keys.

Syntax — `set dot1x wep-rekey {enable | disable}`

- **enable** — Causes the broadcast and multicast keys for WEP to be rotated at an interval set by the **set dot1x wep-rekey-period** for each radio, associated VLAN, and encryption type. The WX generates the new broadcast and multicast keys and pushes the keys to the clients via EAPoL key messages.
- **disable** — WEP broadcast and multicast keys are never rotated.

Defaults — WEP key rotation is enabled, by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Reauthentication is *not* required for WEP key rotation to take place. Broadcast and multicast keys are always rotated at the same time, so all members of a given radio, VLAN, or encryption type receive the new keys at the same time.

Examples — Type the following command to disable WEP key rotation:

```
WX4400# set dot1x wep-rekey disable
success: wep rekeying disabled
```

See Also

- **display dot1x** on page 599
- **set dot1x wep-rekey-period** on page 612

**set dot1x
wep-rekey-period**

Sets the interval for rotating the WEP broadcast and multicast keys.

Syntax — `set dot1x wep-rekey-period seconds`

- *seconds* — Specify a value between 30 and 1,641,600 (19 days).

Defaults — The default is 1800 seconds (30 minutes).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — Type the following command to set the WEP-rekey period to 300 seconds:

```
WX4400# set dot1x wep-rekey-period 300
success: dot1x wep-rekey-period set to 300
```

See Also

- **display dot1x** on page 599
- **set dot1x wep-rekey** on page 611

18

SESSION MANAGEMENT COMMANDS

Use session management commands to display and clear administrative and network user sessions.

Commands by Usage

This chapter presents session management commands alphabetically. Use Table 94 to locate commands in this chapter based on their use.

Table 94 Session Management Commands by Usage

Type	Command
Administrative Sessions	display sessions on page 616
	clear sessions on page 613
Network Sessions	display sessions network on page 620
	clear sessions network on page 615
Mesh AP Sessions	display sessions mesh-ap on page 619

clear sessions

Clears all administrative sessions, or clears administrative console or Telnet sessions.

Syntax — `clear sessions {admin | console | telnet [client [session-id] | mesh-ap [session-id session-id]}`

- **admin** — Clears sessions for all users with administrative access to the WX switch through a Telnet or SSH connection or a console plugged into the switch.
- **console** — Clears sessions for all users with administrative access to the WX switch through a console plugged into the switch.
- **telnet** — Clears sessions for all users with administrative access to the WX switch through a Telnet connection.

- **telnet client** [*session-id*] — Clears all Telnet client sessions from the CLI to remote devices, or clears an individual session identified by session ID.
- **mesh-ap** [*session-id*] — Clears all Mesh AP sessions, or clears an individual Mesh AP session identified by session ID.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To clear all administrator sessions type the following command:

```
WX4400# clear sessions admin
This will terminate manager sessions,
do you wish to continue? (y|n) [n]y
```

To clear all administrative sessions through the console, type the following command:

```
WX4400# clear sessions console
This will terminate manager sessions,
do you wish to continue? (y|n) [n]y
```

To clear all administrative Telnet sessions, type the following command:

```
WX4400# clear sessions telnet
This will terminate manager sessions,
do you wish to continue? (y|n) [n]y
```

To clear Telnet client session 0, type the following command:

```
WX4400# clear sessions telnet client 0
```

See Also

- **display sessions** on page 616

clear sessions network

Clears all network sessions for a specified username or set of usernames, MAC address or set of MAC addresses, virtual LAN (VLAN) or set of VLANs, or session ID.

Syntax — `clear sessions network {user user-glob | mac-addr mac-addr-glob | vlan vlan-glob | session-id local-session-id}`

- **user** *user-glob* — Clears all network sessions for a single user or set of users.

Specify a username, use the double-asterisk wildcard character (******) to specify all usernames, or use the single-asterisk wildcard character (*****) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (@) or a period (.). (For details, see “User Globs” on page 30.)

- **mac-addr** *mac-addr-glob* — Clears all network sessions for a MAC address. Specify a MAC address in hexadecimal numbers separated by colons (:), or use the wildcard character (*****) to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 31.)

- **vlan** *vlan-glob* — Clears all network sessions on a single VLAN or a set of VLANs.

Specify a VLAN name, use the double-asterisk wildcard character (******) to specify all VLAN names, or use the single-asterisk wildcard character (*****) to specify a set of VLAN names up to or following the first delimiter character, either an *at* sign (@) or a period (.). (For details, see “VLAN Globs” on page 32.)

- **session-id** *local-session-id* — Clears the specified 802.1X network session. To find local session IDs, use the `display sessions` command.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The `clear sessions network` command clears network sessions by deauthenticating and, for wireless clients, disassociating them.

Examples — To clear all sessions for MAC address 00:01:02:03:04:05, type the following command:

```
WX4400# clear sessions network mac-addr 00:01:02:03:04:05
```

To clear session 9, type the following command:

```
WX1200# clear sessions network session-id 9
SM Apr 11 19:53:38 DEBUG SM-STATE: localid 9, mac 00:06:25:09:39:5d,
flags 0000012fh, to change state to KILLING
Localid 9, globalid SESSION-9-893249336 moved from ACTIVE to KILLING
(client=00:06:25:09:39:5d)
```

To clear the session of user *Natasha*, type the following command:

```
WX1200# clear sessions network user Natasha
```

To clear the sessions of users whose name begins with the characters *Jo*, type the following command:

```
WX1200# clear sessions network user Jo*
```

To clear the sessions of all users on VLAN *red*, type the following command:

```
WX1200# clear sessions network vlan red
```

See Also

- **display sessions** on page 616
- **display sessions network** on page 620

display sessions

Displays session information and statistics for all users with administrative access to the WX switch, or for administrative users with either console or Telnet access.

Syntax — `display sessions {admin | console | telnet [client]}`

- **admin** — Displays sessions for all users with administrative access to the WX switch through a Telnet or SSH connection or a console plugged into the switch.
- **console** — Displays sessions for all users with administrative access to the WX switch through a console plugged into the switch.

- **telnet** — Displays sessions for all users with administrative access to the WX switch through a Telnet connection.
- **telnet client** — Displays Telnet sessions from the CLI to remote devices.

Defaults — None.

Access — All, except for **display sessions telnet client**, which has enabled access.

History — Introduced in MSS Version 3.0.

Examples — To view information about sessions of administrative users, type the following command:

```
WX4400> display sessions admin
Tty      Username      Time (s)      Type
-----
tty0          3644          Console
tty2      tech           6             Telnet
tty3      sshadmin      381           SSH
```

3 admin sessions

To view information about console users' sessions, type the following command:

```
WX4400> display sessions console
Tty      Username      Time (s)
-----
console          8573
1 console session
```

To view information about Telnet users sessions, type the following command:

```
WX4400> display sessions telnet
Tty      Username      Time (s)
-----
tty2      sea           7395
```

To view information about Telnet client sessions, type the following command:

```
WX4400# display sessions telnet client
Session   Server Address   Server Port   Client Port
-----
0         192.168.1.81    23           48000
1         10.10.1.22     23           48001
```

Table 95 describes the fields of the **display sessions admin**, **display sessions console**, and **display sessions telnet** displays.

Table 95 display sessions admin, display sessions console, and display sessions telnet Output

Field	Description
Tty	The Telnet terminal number, or <i>console</i> for administrative users connected through the console port.
Username	Up to 30 characters of the name of an authenticated user.
Time (s)	Number of seconds the session has been active.
Type	Type of administrative session: <ul style="list-style-type: none"> ▪ Console ▪ SSH ▪ Telnet

Table 96 describes the fields of the **display sessions telnet client** display.

Table 96 display sessions telnet client Output

Field	Description
Session	Session number assigned by MSS when the client session is established.
Server Address	IP address of the remote device.
Server Port	TCP port number of the remote device's TCP server.
Client Port	TCP port number MSS is using for the client side of the session.

See Also

- **clear sessions** on page 613

display sessions mesh-ap

Displays summary or verbose information about Mesh AP sessions on the WX.

Syntax — `display sessions mesh-ap [session-id session-id | verbose]`

- **session-id** *local-session-id* — Displays the specified Mesh AP session. To determine the local session ID for a Mesh AP session, use the **display sessions mesh-ap** command without the **session-id** option.
- **verbose** — Provides detailed output for all Mesh AP sessions.

Defaults — None.

Access — All.

History — Introduced in MSS Version 6.0.

Examples — To view information about Mesh AP sessions, type the following command:

```
WX> display sessions mesh-ap
```

User Name	Sess ID	IP or MAC Address	VLAN Name	Port/ Radio
00:0b:0e:17:bb:3f	2*	1.1.1.3	(none)	L AP 2/2

Table 97 describes the fields of **display sessions mesh-ap** output.

Table 97 display sessions mesh-ap Output

Field	Description
User Name	The MAC address of the authenticated Mesh AP.
Sess ID	Locally unique number that identifies this session. An asterisk (*) next to a session ID indicates that the session is fully active.
IP or MAC Address	IP address of the Mesh AP.
VLAN Name	Name of the VLAN associated with the session.
Port/Radio	Number of the port and radio through which the Mesh AP is accessing this session.

See also “clear sessions” on page 613

display sessions network

Displays summary or verbose information about all network sessions, or network sessions for a specified username or set of usernames, MAC address or set of MAC addresses, VLAN or set of VLANs, or session ID.

Syntax — display sessions network

```
[user user-glob | mac-addr mac-addr-glob | ssid ssid-name
vlan vlan-glob | session-id session-id | wired] [verbose]
```

- **user** *user-glob* — Displays all network sessions for a single user or set of users.

Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an *at* sign (@) or a period (.). (For details, see “User Globs” on page 30.)

- **mac-addr** *mac-addr-glob* — Displays all network sessions for a MAC address. Specify a MAC address in hexadecimal numbers separated by colons (:).

Or use the wildcard character (*) to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 31.)

- **ssid** *ssid-name* — Displays all network sessions for an SSID.
- **vlan** *vlan-glob* — Displays all network sessions on a single VLAN or a set of VLANs.

Specify a VLAN name, use the double-asterisk wildcard character (**) to specify all VLAN names, or use the single-asterisk wildcard character (*) to specify a set of VLAN names up to or following the first delimiter character, either an *at* sign (@) or a period (.). (For details, see “VLAN Globs” on page 32.)

- **session-id** *local-session-id* — Displays the specified network session. To find local session IDs, use the **display sessions** command. The **verbose** option is not available with this form of the **display sessions network** command.
- **wired** — Displays all network sessions on wired authentication ports.
- **verbose** — Provides detailed output for all network sessions or ones displayed by username, MAC address, or VLAN name.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0. Output added to the **display network sessions verbose** command to indicate the user's authorization attributes and whether they were supplied through AAA or through configured SSID defaults in a service profile in MSS Version 4.1.

Usage — MSS displays information about network sessions in three types of displays. See the following tables for field descriptions.

- **Summary display** — See Table 98 on page 623.
- **Verbose display** — See Table 99 on page 624.
- **display sessions network session-id** display — See Table 100 on page 626.

Examples — To display summary information for all network sessions, type **display sessions network**. For example:

```
WX1200# display sessions network
User                               Sess IP or MAC          VLAN              Port/
Name                               ID   Address            Name              Radio
-----
EXAMPLE\Natasha                    4*  10.10.40.17        vlan-eng          3/1
host/laptop11.exmpl.com            6*  10.10.40.16        vlan-eng          3/2
nin@exmpl.com                      539* 10.10.40.17        vlan-eng          1/1
EXAMPLE\hosni                      302* 10.10.40.10        vlan-eng          3/1
                                     563  00:0b:be:15:46:56  (none)           1/2
jose@exmpl.com                     380* 10.30.40.8         vlan-eng          1/1
00:30:65:16:8d:69                  443* 10.10.40.19        vlan-wep          3/1
EXAMPLE\Geetha                     459* 10.10.40.18        vlan-eng          3/2
8 sessions total
```

The following command displays summary information about the sessions for MAC address 00:05:5d:7e:98:1a:

```
WX1200# display sessions network mac-addr 00:05:5d:7e:98:1a
User                               Sess IP or MAC          VLAN              Port/
Name                               ID   Address            Name              Radio
-----
EXAMPLE\Havel                      13* 10.10.10.40        vlan-eng          1/2
```

The following command displays summary information about all the sessions of users whose names begin with *E*:

```
WX1200# display sessions network user E*
User          Sess  IP or MAC      VLAN      Port/
Name          ID   Address        Name       Radio
-----
EXAMPLE\Singh      12*  10.10.10.30   vlan-eng   3/2
EXAMPLE\Havel     13*  10.10.10.40   vlan-eng   1/2
2 sessions match criteria (of 3 total)
```

(Table 98 on page 623 describes the summary displays of **display sessions network** commands.)

The following command displays detailed (verbose) session information about user *nin@example.com*:

```
WX1200# display sessions network user nin@example.com verbose
User          Sess  IP or MAC      VLAN      Port/
Name          ID   Address        Name       Radio
-----
nin@example.com      5*  10.20.30.40   vlan-eng   1/1
Client MAC: 00:02:2d:6e:ab:a5  GID: SESS-5-000430-686792-d8b3c564
State: ACTIVE      (prev AUTHORIZED)
now on: WX 192.168.12.7, AP/radio 1/1, AP 00:0b:0e:00:05:fe, as of 00:23:32 ago
1 sessions match criteria (of 10 total)
```

The following command displays verbose output about the sessions of all current network users:

```
WX1200# display sessions network verbose
User          Sess  IP or MAC      VLAN      Port/
Name          ID   Address        Name       Radio
-----
SHUTTLE2\exmpl      6*  10.3.8.55     default    3/1
Client MAC: 00:06:25:13:08:33  GID: SESS-4-000404-98441-c807c14b
State: ACTIVE      (prev AUTHORIZED)
now on: WX 10.3.8.103, AP/radio 3/1, AP 00:0b:0e:ff:00:3a, as of
00:00:24 ago
  from: WX 10.3.8.103, AP/radio 6/1, AP 00:0b:0e:00:05:d7, as of
00:01:07 ago
  from: WX 10.3.8.103, AP/radio 3/1, AP 00:0b:0e:ff:00:3a, as of
00:01:53 ago

Vlan-Name=default (service-profile)
Service-Type=2 (service-profile)
End-Date=52/06/07-08:57 (AAA)
```

Start-Date=05/04/11-10:00 (AAA)

1 sessions total

(Table 99 on page 624 describes the additional fields of the **verbose** output of **display sessions network** commands.)

The following command displays information about network session 27:

```
WX1200# display sessions network session-id 27
Global Id: SESS-27-000430-835586-58dfe5a
State: ACTIVE
Port/Radio: 3/1
MAC Address: 00:00:2d:6f:44:77
User Name: EXAMPLE Natasha
IP Address: 10.10.40.17
Vlan Name: vlan-eng
Tag: 1
Session Timeout: 1800
Authentication Method: PEAP, using server 10.10.70.20
Session statistics as updated from AP:
Unicast packets in: 653
Unicast bytes in: 46211
Unicast packets out: 450
Unicast bytes out: 50478
Multicast packets in: 317
Multicast bytes in: 10144
Number of packets with encryption errors: 0
Number of bytes with encryption errors: 0
Last packet data rate: 2
Last packet signal strength: -67 dBm
Last packet data S/N ratio: 55
```

Table 98 describes the output of this command. For descriptions of the fields of **display sessions network session-id** output, see Table 100 on page 626.

Table 98 display sessions network (summary) Output

Field	Description
User Name	Up to 30 characters of the name of the authenticated user of this session.

Table 98 display sessions network (summary) Output

Field	Description
Sess ID	Locally unique number that identifies this session. An asterisk (*) next to the session ID indicates fully active sessions.
IP or MAC Address	IP address of the session user, or the user's MAC address if the user has not yet received an IP address.
VLAN Name	Name of the VLAN associated with the session.
Port/Radio	Number of the port and radio through which the user is accessing this session.

Table 99 Additional display sessions network verbose Output

Field	Description
Client MAC	MAC address of the session user.
GID	Global session ID, a unique session number within a Mobility Domain.

Table 99 Additional display sessions network verbose Output (continued)

Field	Description
State	<p>Status of the session:</p> <ul style="list-style-type: none"> ▪ AUTH, ASSOC REQ — Client is being associated by the 802.1X protocol. ▪ AUTH AND ASSOC — Client is being associated by the 802.1X protocol, and the user is being authenticated. ▪ AUTHORIZING — User has been authenticated (for example, by the 802.1X protocol and an AAA method), and is entering AAA authorization. ▪ AUTHORIZED — User has been authorized by an AAA method. ▪ ACTIVE — User's AAA attributes have been applied, and the user is active on the network. ▪ DEASSOCIATED — One of the following: <ul style="list-style-type: none"> Wireless client has sent the WX switch a disassociate message. User associated with one of the current WX switch's MAP access points has appeared at another WX switch in the Mobility Domain. ▪ ROAMING AWAY — The W switch has been sent a request to transfer the user, who is roaming, to another WX switch. ▪ STATUS UPDATED — WX switch is receiving a final update from a MAP access point about the user, who has roamed away. ▪ WEB_AUTHING — User is being authenticated by WebAAA. ▪ WIRED AUTH'ING — User is being authenticated by the 802.1X protocol on a wired authentication port. ▪ KILLING — User's session is being cleared, because of 802.1X authentication failure, entry of a clear command, or some other event.
now on	IP address and port and radio numbers of the session's current WX switch, the MAC address of the MAP access point, and the last update time.
from	IP address and port and radio numbers of the session's previous WX switch, the MAC address of the MAP access point, and the last update time. Up to six roaming events are tracked in this display.
Vlan-Name Service-Type End-Date Start-Date	Authorization attributes for the user and how they were assigned. The authorization attributes can be assigned either by a RADIUS server or the local database (indicated in the output by AAA), or by SSID default settings in the service profile the user used to gain access to the network (indicated in the output by service-profile).

Table 100 display sessions network session-id Output

Field	Description
Global Id	A unique session identifier within the Mobility Domain.
State	<p>Status of the session:</p> <ul style="list-style-type: none"> ■ AUTH, ASSOC REQ — Client is being associated by the 802.1X protocol. ■ AUTH AND ASSOC — Client is being associated by the 802.1X protocol, and the user is being authenticated. ■ AUTHORIZING — User has been authenticated (for example, by the 802.1X protocol and an AAA method), and is entering AAA authorization. ■ AUTHORIZED — User has been authorized by an AAA method. ■ ACTIVE — User's AAA attributes have been applied, and the user is active on the network. ■ DEASSOCIATED — One of the following: <ul style="list-style-type: none"> Wireless client has sent the WX switch a disassociate message. User associated with one of the current WX switch's MAP access points has appeared at another WX switch in the Mobility Domain. ■ ROAMING AWAY — The WX switch has been sent a request to transfer the user, who is roaming, to another WX switch. ■ STATUS UPDATED — WX switch is receiving a final update from an MAP access point about the user, who has roamed away. ■ WEB_AUTHING — User is being authenticated by WebAAA. ■ WIRED AUTH'ING — User is being authenticated by the 802.1X protocol on a wired authentication port. ■ KILLING — User's session is being cleared, because of 802.1X authentication failure, entry of a clear command, or some other event.
Port/Radio	Number of the port and radio through which the user is accessing this session.
MAC address	MAC address of the session user.
User Name	Name of the authenticated user of this session
IP Address	IP address of the session user.
Vlan Name	Name of the VLAN associated with the session.
Tag	System-wide supported VLAN tag type.
Session Timeout	Assigned session timeout in seconds.

Table 100 display sessions network session-id Output (continued)

Field	Description
Authentication Method	Extensible Authentication Protocol (EAP) type used to authenticate the session user, and the IP address of the authentication server.
Session statistics as updated from AP	Time the session statistics were last updated from the MAP access point, in seconds since a fixed standard date and time.
Unicast packets in	Total number of unicast packets received from the user by the WX (64-bit counter).
Unicast bytes in	Total number of unicast bytes received from the user by the WX (64-bit counter).
Unicast packets out	Total number of unicast packets sent by the WX to the user (64-bit counter).
Unicast bytes out	Total number of unicast bytes sent by the WX to the user (64-bit counter).
Multicast packets in	Total number of multicast packets received from the user by the WX (64-bit counter).
Multicast bytes in	Total number of multicast bytes received from the user by the WX (64-bit counter).
Number of packets with encryption errors	Total number of decryption failures.
Number of bytes with encryption errors	Total number of bytes with decryption errors.
Last packet data rate	Data transmit rate, in megabits per second (Mbps), of the last packet received by the MAP access point.
Last packet signal strength	Signal strength, in decibels referred to 1 milliwatt (dBm), of the last packet received by the MAP access point.
Last packet data S/N ratio	Signal-to-noise ratio of the last packet received by the MAP access point.

See Also

- **clear sessions network** on page 615

19

RF DETECTION COMMANDS

MSS automatically performs RF detection scans on enabled and disabled radios to detect rogue access points. A rogue access point is a BSSID (MAC address associated with an SSID) that does not belong to a 3Com switch and is not a member of the ignore list configured on the seed switch of the Mobility Domain. The ignore list is a list of third-party (*friendly*) BSSIDs that are not rogues.

MSS can issue countermeasures against rogue devices to prevent clients from being able to use them.

You can configure RF detection parameters only on the seed switch of a Mobility Domain.

Commands by Usage

This chapter presents RF detection commands alphabetically. Use Table 101 to locate the commands in this chapter based on their use.

Table 101 RF Detection Commands by Usage

Type	Command
Rogue Information	display rfdetect clients on page 637
	display rfdetect mobility-domain on page 644
	display rfdetect data on page 642
	display rfdetect visible on page 650
	display rfdetect counters on page 640
Countermeasures	display rfdetect countermeasures on page 639
Permitted Vendor List	set rfdetect vendor-list on page 660
	display rfdetect vendor-list on page 649

Table 101 RF Detection Commands by Usage (continued)

Type	Command
	clear rfdetect vendor-list on page 633
Permitted SSID List	set rfdetect ssid-list on page 659
	display rfdetect ssid-list on page 649
	clear rfdetect ssid-list on page 632
Client Black List	set rfdetect black-list on page 654
	display rfdetect black-list on page 636
	clear rfdetect black-list on page 631
Attack List	set rfdetect attack-list on page 653
	display rfdetect attack-list on page 635
	clear rfdetect attack-list on page 630
Ignore List	set rfdetect ignore on page 656
	display rfdetect ignore on page 644
	clear rfdetect ignore on page 631
MAP Signatures	set rfdetect signature on page 658
Log Messages	set rfdetect log on page 657
WX-to-Client RF Link	rfping on page 634

clear rfdetect attack-list

Removes a MAC address from the attack list.

Syntax — `clear rfdetect attack-list mac-addr`

- *mac-addr* — MAC address you want to remove from the attack list.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command clears MAC address 11:22:33:44:55:66 from the attack list:

```
wx4400# clear rfdetect attack-list 11:22:33:44:55:66
success: 11:22:33:44:55:66 is no longer in attacklist.
```

See Also

- **clear rfdetect attack-list** on page 630
- **display rfdetect attack-list** on page 635

**clear rfdetect
black-list**

Removes a MAC address from the client black list.

Syntax — `clear rfdetect black-list mac-addr`

- *mac-addr* — MAC address you want to remove from the black list.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command removes MAC address 11:22:33:44:55:66 from the black list:

```
WX1200# clear rfdetect black-list 11:22:33:44:55:66
success: 11:22:33:44:55:66 is no longer blacklisted.
```

See Also

- **display rfdetect black-list** on page 636
- **set rfdetect black-list** on page 654

**clear rfdetect
ignore**

Removes a device from the ignore list for RF scans. MSS does not generate log messages or traps for the devices in the ignore list.

Syntax — `clear rfdetect ignore mac-addr`

- *mac-addr* — Basic service set identifier (BSSID), which is a MAC address, of the device to remove from the ignore list.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes BSSID *aa:bb:cc:11:22:33* from the ignore list for RF scans:

```
WX1200# clear rfdetect ignore aa:bb:cc:11:22:33
success: aa:bb:cc:11:22:33 is no longer ignored.
```

See Also

- **display rfdetect ignore** on page 644
- **set rfdetect ignore** on page 656

clear rfdetect ssid-list

Removes an SSID from the permitted SSID list.

Syntax — `clear rfdetect ssid-list ssid-name`

- *ssid-name* — SSID name you want to remove from the permitted SSID list.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command clears SSID *mycorp* from the permitted SSID list:

```
WX1200# clear rfdetect ssid-list mycorp
success: mycorp is no longer in ssid-list.
```

See Also

- **display rfdetect ssid-list** on page 649
- **set rfdetect ssid-list** on page 659

**clear rfdetect
vendor-list**

Removes an entry from the permitted vendor list.

Syntax — `clear rfdetect vendor-list {client | ap} mac-addr | all`

- **client | ap** — Specifies whether the entry is for an AP brand or a client brand.
- **mac-addr | all** — Organizationally Unique Identifier (OUI) to remove.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command removes client OUI aa:bb:cc:00:00:00 from the permitted vendor list:

```
WX4400# clear rfdetect vendor-list client aa:bb:cc:00:00:00
success: aa:bb:cc:00:00:00 is no longer in client
vendor-list.
```

See Also

- **display rfdetect vendor-list** on page 649
- **set rfdetect vendor-list** on page 660

rfping

Provides information about the RF link between the WX and the client based on sending test packets to the client.

- **Syntax** — `rfping {mac mac-addr | session-id session-id}`
- *mac-addr* — Tests the RF link between the WX and the client with the specified MAC address.
- *session-id* — Tests the RF link between the WX and the client with the specified local session ID.

Defaults — None.

Access — Enabled.

History — Version 4.2 Command introduced. Version 6.0 Name of command changed from **test rflink** to **rfping**.

Usage — Use this command to send test packets to a specified client. The output of the command indicates the number of test packets received and acknowledged by the client, as well as the client's signal strength and signal-to-noise ratio.

Examples — The following command tests the RF link between the WX switch and the client with MAC address 00:0e:9b:bf:ad:13:

```
WX# rfping mac 00:0e:9b:bf:ad:13
RF-Link Test to 00:0e:9b:bf:ad:13 :
Session-Id: 2
Packets Sent  Packets Rcvd  RSSI      SNR      RTT (micro-secs)
-----
                20             20      -68       26       976
```

Table 83 describes the fields in this display.

Table 102 rfping Output

Field	Description
Packets Sent	The number of test packets sent from the WX switch to the client.
Packets Rcvd	The number of test packets acknowledged by the client.

Table 102 rfping Output (continued)

Field	Description
RSSI	Received signal strength indication (RSSI) of the strength of the RF signal from the client, in decibels referred to 1 milliwatt (dBm).
SNR	Signal-to-noise ratio (SNR), in decibels (dB), of the data received from the client.
RTT (micro-secs)	The round-trip time, in microseconds, for the client response to the test packets.

See Also

- **display rfdetect data** on page 642
- **display rfdetect visible** on page 650

display rfdetect attack-list

Displays information about the MAC addresses in the attack list.

Syntax — `display rfdetect attack-list`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following example shows the attack list on WX switch:

```
WX1200# display rfdetect attack-list
Total number of entries: 1
  Attacklist MAC      Port/Radio/Chan  RSSI      SSID
-----
11:22:33:44:55:66 ap 2/1/11         -53      rogue-ssid
```

See Also

- **clear rfdetect attack-list** on page 630
- **set rfdetect attack-list** on page 653

**display rfdetect
black-list**

Displays information about the clients in the client black list.

Syntax — `display rfdetect black-list`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following example shows the client black list on WX switch:

```
WX1200# display rfdetect black-list
Total number of entries: 1
  Blacklist MAC          Type          Port  TTL
-----
11:22:33:44:55:66  configured    -      -
11:23:34:45:56:67  assoc req flood  3      25
```

See Also

- **clear rfdetect black-list** on page 631
- **set rfdetect black-list** on page 654

display rfdetect clients

Displays the wireless clients detected by a WX switch.

Syntax — `display rfdetect clients [mac mac-addr]`

mac mac-addr — Displays detailed information for a specific client.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command shows information about all wireless clients detected by a WX switch's MAPs:

```
WX4400# display rfdetect clients
Total number of entries: 30
Client MAC          Client          AP MAC          AP          Port/Radio      NoL Type      Last
                   Vendor          Vendor          Vendor          /Channel        seen
-----
00:03:7f:bf:16:70  Unknown          Unknown          ap          1/1/6           1 intfr 207
00:04:23:77:e6:e5  Intel            Unknown          ap          1/1/2           1 intfr 155
00:05:5d:79:ce:0f  D-Link           Unknown          ap          1/1/149         1 intfr 87
00:05:5d:7e:96:a7  D-Link           Unknown          ap          1/1/149         1 intfr 117
00:05:5d:7e:96:ce  D-Link           Unknown          ap          1/1/157         1 intfr 162
00:05:5d:84:d1:c5  D-Link           Unknown          ap          1/1/1           1 intfr 52
```

The following command displays more details about a specific client:

```
WX4400# display rfdetect clients mac 00:0c:41:63:fd:6d
Client Mac Address: 00:0c:41:63:fd:6d, Vendor: Linksys
Port: ap 1, Radio: 1, Channel: 11, RSSI: -82, Rate: 2, Last Seen (secs ago):
84
Bssid: 00:0b:0e:01:02:00, Vendor: 3Com, Type: intfr, Dst: ff:ff:ff:ff:ff:ff
Last Rogue Status Check (secs ago): 3
```

The first line lists information for the client. The other lines list information about the most recent 802.11 packet detected from the client.

Table 103 and Table 104 describe the fields in these displays.

Table 103 display rfdetect clients Output

Field	Description
Client MAC	MAC address of the client.
Client Vendor	Company that manufactures or sells the client.
AP MAC	MAC address of the radio with which the rogue client is associated.
AP Vendor	Company that manufactures or sells the AP with which the rogue client is associated.
Port/Radio/Channel	Port number, radio number, and channel number of the radio that detected the rogue.
NoL	Number of listeners. This is the number of MAP radios that detected the rogue client.
Type	Classification of the rogue device: <ul style="list-style-type: none"> ■ rogue—Wireless device that is on the network but is not supposed to be on the network. ■ intrfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with MAP radios. ■ known—Device that is a legitimate member of the network.
Last seen	Number of seconds since a MAP radio last detected 802.11 packets from the device.

Table 104 display rfdetect clients mac Output

Field	Description
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal detected by the MAP radio, in decibels referred to 1 milliwatt (dBm).
Rate	The data rate of the client.
Last Seen	Number of seconds since a MAP radio last detected 802.11 packets from the device.
BSSID	MAC address of the SSID with which the rogue client is associated.
Vendor	Company that manufactures or sells the AP with which the rogue client is associated.

Table 104 display rfdetect clients mac Output (continued)

Field	Description
Typ	Classification of the rogue device: <ul style="list-style-type: none"> ▪ rogue—Wireless device that is on the network but is not supposed to be on the network. ▪ intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with MAP radios. ▪ known—Device that is a legitimate member of the network.
Dst	MAC addressed to which the last 802.11 packet detected from the client was addressed.
Last Rogue Status Check	Number of seconds since the WX switch looked on the air for the AP with which the rogue client is associated. The switch looks for the client's AP by sending a packet from the wired side of the network addressed to the client, and watching the air for a wireless packet containing the client's MAC address.

display rfdetect countermeasures

Displays the current status of countermeasures against rogues in the Mobility Domain.

Syntax — `display rfdetect countermeasures`

Defaults — None.

Access — Enabled.

History — Output no longer lists rogues for which countermeasures have not been started in MSS Version 4.0.

Usage — This command is valid only on the seed switch of the Mobility Domain.

Examples — The following example displays countermeasures status for the Mobility Domain:

```
WX4400# display rfdetect countermeasures
Total number of entries: 190
Rogue MAC          Type  Countermeasures   WX-IPaddr   Port/Radio
                   Radio Mac                                     /Channel
-----
00:0b:0e:00:71:c0 intfr  00:0b:0e:44:55:66 10.1.1.23   ap 4/1/6
00:0b:0e:03:00:80 rogue  00:0b:0e:11:22:33 10.1.1.23   ap 2/1/11
```

Table 105 describes the fields in this display.

Table 105 display rfdetect countermeasures Output

Field	Description
Rogue MAC	BSSID of the rogue.
Type	Classification of the rogue device: <ul style="list-style-type: none"> ▪ rogue—Wireless device that is on the network but is not supposed to be on the network. ▪ intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with MAP radios. ▪ known—Device that is a legitimate member of the network.
Countermeasures Radio MAC	MAC address of the 3Com radio sending countermeasures against the rogue.
WX-IPaddr	System IP address of the WX switch that is managing the MAP that is sending or will send countermeasures.
Port/Radio/Channel	Port number, radio number, and channel number of the countermeasures radio.

See Also

- **set radio-profile countermeasures** on page 410

display rfdetect counters

Displays statistics for rogue and Intrusion Detection System (IDS) activity detected by the MAPs managed by a WX switch.

Syntax — `display rfdetect counters`

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.0.

Examples — The following command shows counters for rogue activity detected by a WX switch:

```
WX4400# display rfdetect counters
```

Type	Current	Total
Rogue access points	0	0
Interfering access points	139	1116
Rogue 802.11 clients	0	0
Interfering 802.11 clients	4	347
802.11 adhoc clients	0	1
Unknown 802.11 clients	20	965
Interfering 802.11 clients seen on wired network	0	0
802.11 probe request flood	0	0
802.11 authentication flood	0	0
802.11 null data flood	0	0
802.11 mgmt type 6 flood	0	0
802.11 mgmt type 7 flood	0	0
802.11 mgmt type d flood	0	0
802.11 mgmt type e flood	0	0
802.11 mgmt type f flood	0	0
802.11 association flood	0	0
802.11 reassociation flood	0	0
802.11 disassociation flood	0	0
Weak wep initialization vectors	0	0
Spoofed access point mac-address attacks	0	0
Spoofed client mac-address attacks	0	0
Ssid masquerade attacks	1	12
Spoofed deauthentication attacks	0	0
Spoofed disassociation attacks	0	0
Null probe responses	626	11380
Broadcast deauthentications	0	0
FakeAP ssid attacks	0	0
FakeAP bssid attacks	0	0
Netstumbler clients	0	0
Wellenreiter clients	0	0
Active scans	1796	4383
Wireless bridge frames	196	196
Adhoc client frames	8	0
Access points present in attack-list	0	0
Access points not present in ssid-list	0	0
Access points not present in vendor-list	0	0
Clients not present in vendor-list	0	0
Clients added to automatic black-list	0	0

display rfdetect data

Displays all the BSSIDs detected by an individual WX switch during an RF detection scan. The data includes BSSIDs transmitted by other 3Com radios as well as by third-party access points.

Syntax — `display rfdetect data`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. Vendor, Type, and Flag fields added in MSS Version 4.0.

Usage — You can enter this command on any WX switch in the Mobility Domain. The output applies only to the switch on which you enter the command. To display all devices that a specific 3Com radio has detected, even if the radio is managed by another WX switch, use the **display rfdetect visible** command.

To display rogue information for the entire Mobility Domain, use the **display rfdetect mobility-domain** command on the seed switch.

Only one MAC address is listed for each 3Com radio, even if the radio is beaconing multiple SSIDs.

Examples — The following command shows the devices detected by this WX switch during the most recent RF detection scan:

```
WX1200# display rfdetect data
Total number of entries: 7
      BSSID          Port/Rad   Chan   RSSI Age  SSID
-----
00:06:25:09:39:4a   5/1        3  0    15 rack29-hostap
00:06:25:51:e9:ff   4/1        10 -85   15 Arrow
00:06:25:51:e9:ff   5/1        10 -84   15 Arrow
00:0b:0e:00:00:00   4/1        1  -78   15 gary-eng
00:0b:0e:00:02:00   4/1        11 -76   15 public
00:0b:0e:00:02:00   5/1        11 -74   15 public
00:0b:0e:00:02:01   4/1        56 -68   15 public
```

Table 106 describes the fields in this display.

Table 106 display rfdetect data Output

Field	Description
BSSID	BSSID detected by a MAP radio on this WX switch.
Vendor	Company that manufactures or sells the rogue device.
Type	Classification of the rogue device: <ul style="list-style-type: none"> ▪ rogue—Wireless device that is not supposed to be on the network. The device has an entry in a WX switch's FDB and is therefore on the network. ▪ intrfr—Wireless device that is not part of your network but is not a rogue. The device does not have an entry in a WX switch's FDB and is not actually on the network, but might be causing RF interference with MAP radios. ▪ known—Device that is a legitimate member of the network.
Port/Radio/Channel	Port number, radio number, and channel number of the radio that detected the rogue.
Flags	Classification and encryption information for the rogue: <ul style="list-style-type: none"> ▪ The i, a, or u flag indicates the classification. ▪ The other flags indicate the encryption used by the rogue. For flag definitions, see the key in the command output.
RSSI	Received signal strength indication (RSSI) — the strength of the RF signal detected by the MAP radio, in decibels referred to 1 milliwatt (dBm).
Age	Age of the rogue listing, in seconds. Rogues age out of the rogue list after one minute.
SSID	Service set identifier (SSID) associated with the BSSID.

See Also

- **display rfdetect mobility-domain** on page 644
- **display rfdetect visible** on page 650

display rfdetect ignore

Displays the BSSIDs of third-party devices that MSS ignores during RF scans. MSS does not generate log messages or traps for the devices in the ignore list.

Syntax — `display rfdetect ignore`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following example displays the list of ignored devices:

```
WX4400# display rfdetect ignore
Total number of entries: 2
  Ignore MAC
-----
aa:bb:cc:11:22:33
aa:bb:cc:44:55:66
```

See Also

- **clear rfdetect ignore** on page 631
- **set rfdetect ignore** on page 656

display rfdetect mobility-domain

Displays the rogues detected by all WX switches in the Mobility Domain during RF detection scans.

Syntax — `display rfdetect mobility-domain`
`[ssid ssid-name | bssid mac-addr]`

- **ssid ssid-name** — Displays rogues that are using the specified SSID.
- **bssid mac-addr** — Displays rogues that are using the specified BSSID.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. **Bssid** and **ssid** options added; Vendor, Type and Flag fields added in MSS Version 4.0.

Usage — This command is valid only on the seed switch of the Mobility Domain. To display rogue information for an individual switch, use the **display rfdetect data** command on that switch.

Only rogues are listed. To display all devices detected, including 3Com radios, use the **display rfdetect data** command.

Examples — The following example displays information about the BSSIDs detected in the Mobility Domain managed by the seed switch:

```
WX1200# display rfdetect mobility-domain
Total number of entries: 194
Flags: i = infrastructure, a = ad-hoc, u = unresolved
       c = CCMP, t = TKIP, l = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
BSSID      Vendor      Type  Flags  SSID
-----
00:07:50:d5:cc:91      Cisco  intf  i----w  r27-cisco1200-2
00:07:50:d5:dc:78      Cisco  intf  i----w  r116-cisco1200-2
00:09:b7:7b:8a:54      Cisco  intf  i-----
00:0a:5e:4b:4a:c0      3Com   intf  i-----  public
00:0a:5e:4b:4a:c2      3Com   intf  i----w  3Comwlan
00:0a:5e:4b:4a:c4      3Com   intf  ic----  3Com-ccmp
00:0a:5e:4b:4a:c6      3Com   intf  i----w  3Com-tkip
00:0a:5e:4b:4a:c8      3Com   intf  i----w  3Com-voip
00:0a:5e:4b:4a:ca      3Com   intf  i-----  3Com-webaaa
...
```

The lines in this display are compiled from data from multiple listeners (MAP radios). If an item has the value *unresolved*, not all listeners agree on the value for that item. Generally, an unresolved state occurs only when a MAP or a Mobility Domain is still coming up, and lasts only briefly.

The following command displays detailed information for rogues using SSID *3com-webaaa*.

```
WX1200# display rfdetect mobility-domain ssid 3Com-webaaa
BSSID: 00:0a:5e:4b:4a:ca Vendor: 3Com SSID: 3Com-webaaa
Type: intf Adhoc: no Crypto-types: clear

WX-IPaddress: 10.8.121.102 Port/Radio/Ch: 3/1/11 Mac:
00:0b:0e:00:0a:6a
Device-type: interfering Adhoc: no Crypto-types: clear
RSSI: -85 SSID: 3Com-webaaa

BSSID: 00:0b:0e:00:7a:8a Vendor: 3Com SSID: 3com-webaaa
Type: intf Adhoc: no Crypto-types: clear
```

```

    WX-IPaddress: 10.8.121.102 Port/Radio/Ch: 3/1/1 Mac:
00:0b:0e:00:0a:6a
    Device-type: interfering Adhoc: no Crypto-types: clear
    RSSI: -75 SSID: 3Com-webaaa

    WX-IPaddress: 10.3.8.103 Port/Radio/Ch: ap 1/1/1 Mac:
00:0b:0e:76:56:82
    Device-type: interfering Adhoc: no Crypto-types: clear
    RSSI: -76 SSID: 3Com-webaaa

```

Two types of information are shown. The lines that are not indented show the BSSID, vendor, and information about the SSID. The indented lines that follow this information indicate the listeners (MAP radios) that detected the SSID. Each set of indented lines is for a separate MAP listener.

In this example, two BSSIDs are mapped to the SSID. Separate sets of information is shown for each of the BSSIDs, and information about the listeners for each BSSID are shown.

The following command displays detailed information for a BSSID.

```

WX1200# display rfdetect mobility-domain bssid
00:0b:0e:00:04:d1
BSSID: 00:0b:0e:00:04:d1 Vendor: Cisco SSID: notmycorp
Type: rogue Adhoc: no Crypto-types: clear

    WX-IPaddress: 10.8.121.102 Port/Radio/Ch: 3/2/56 Mac:
00:0b:0e:00:0a:6b
    Device-type: rogue Adhoc: no Crypto-types: clear
    RSSI: -72 SSID: notmycorp

    WX-IPaddress: 10.3.8.103 Port/Radio/Ch: ap 1/1/157 Mac:
00:0b:0e:76:56:82
    Device-type: rogue Adhoc: no Crypto-types: clear
    RSSI: -72 SSID: notmycorp

```

Table 107 and Table 108 describe the fields in these displays.

Table 107 display rfdetect mobility-domain Output

Field	Description
BSSID	MAC address of the SSID used by the detected device.
Vendor	Company that manufactures or sells the rogue device.
Type	Classification of the rogue device: <ul style="list-style-type: none"> ■ rogue—Wireless device that is not supposed to be on the network. The device has an entry in a WX switch’s FDB and is therefore on the network. ■ intfr—Wireless device that is not part of your network but is not a rogue. The device does not have an entry in a WX switch’s FDB and is not actually on the network, but might be causing RF interference with MAP radios. ■ known—Device that is a legitimate member of the network.
Flags	Classification and encryption information for the rogue: <ul style="list-style-type: none"> ■ The i, a, or u flag indicates the classification. ■ The other flags indicate the encryption used by the rogue. For flag definitions, see the key in the command output.
SSID	SSID used by the detected device.

Table 108 display rfdetect mobility-domain ssid or bssid Output

Field	Description
BSSID	MAC address of the SSID used by the detected device.
Vendor	Company that manufactures or sells the rogue device.
SSID	SSID used by the detected device.
Type	Classification of the rogue device: <ul style="list-style-type: none"> ■ rogue—Wireless device that is on the network but is not supposed to be on the network. ■ intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with MAP radios. ■ known—Device that is a legitimate member of the network.
Adhoc	Indicates whether the rogue is an infrastructure rogue (is using an AP) or is operating in ad-hoc mode.

Table 108 display rfdetect mobility-domain ssid or bssid Output (continued)

Field	Description
Crypto-Types	Encryption type: clear (no encryption) ccmp tkip wep104 (WPA 104-bit WEP) wep40 (WPA 40-bit WEP) wep (non-WPA WEP)
WX-IPaddress	System IP address of the WX switch that detected the rogue.
Port/Radio/Channel	Port number, radio number, and channel number of the radio that detected the rogue.
Mac	MAC address of the radio that detected the rogue.
Device-type	Device type detected by the MAP radio.
Adhoc	Ad-hoc status (yes or no) detected by the MAP radio.
Crypto-Types	Encryption type detected by the MAP radio.
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal detected by the MAP radio, in decibels referred to 1 milliwatt (dBm).
SSID	SSID mapped to the BSSID.

See Also

- **display rfdetect data** on page 642
- **display rfdetect visible** on page 650

**display rfdetect
ssid-list**

Displays the entries in the permitted SSID list.

Syntax — `display rfdetect ssid-list`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following example shows the permitted SSID list on WX switch:

```
WX4400# display rfdetect ssid-list
Total number of entries: 3
      SSID
-----
      mycorp
      corporate
      guest
```

See Also

- **clear rfdetect ssid-list** on page 632
- **set rfdetect ssid-list** on page 659

**display rfdetect
vendor-list**

Displays the entries in the permitted vendor list.

Syntax — `display rfdetect vendor-list`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following example shows the permitted vendor list on WX switch:

```
WX1200# display rfdetect vendor-list
Total number of entries: 1
          OUI           Type
-----
aa:bb:cc:00:00:00 client
11:22:33:00:00:00 ap
```

See Also

- **clear rfdetect vendor-list** on page 633
- **set rfdetect vendor-list** on page 660

display rfdetect visible

Displays the BSSIDs discovered by a specific 3Com radio. The data includes BSSIDs transmitted by other 3Com radios as well as by third-party access points.

Syntax — **display rfdetect visible** *mac-addr*

Syntax — **display rfdetect visible ap** *mp-num* [**radio** {**1** | **2**}]

- *mac-addr* — Base MAC address of the 3Com radio.
 - Note:** To display the base MAC address of a 3Com radio, use the **display ap status** command.
- *mp-num* — Port connected to the MAP access point for which to display neighboring BSSIDs.
- *dap-num* — Number of a Distributed MAP for which to display neighboring BSSIDs.
- **radio 1** — Shows neighbor information for radio 1.
- **radio 2** — Shows neighbor information for radio 2. (This option does not apply to single-radio models.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — If a 3Com radio is supporting more than one SSID, each of the corresponding BSSIDs is listed separately.

To display rogue information for the entire Mobility Domain, use the **display rfdetect mobility-domain** command on the seed switch.

Examples — The following command displays the devices detected by 3Com radio 00:0b:0e:00:0a:6a:

```
WX1200# display rfdetect visible 00:0b:0e:00:0a:6a ap 3 radio 1
Total number of entries: 104
Flags: i = infrastructure, a = ad-hoc
       c = CCMP, t = TKIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
Transmit MAC      Vendor  Type  Ch  RSSI  Flags  SSID
-----
00:07:50:d5:cc:91  Cisco  intf  6   -60  i----w  r27-cisco1200-2
00:07:50:d5:dc:78  Cisco  intf  6   -82  i----w  r116-cisco1200-2
00:09:b7:7b:8a:54  Cisco  intf  2   -54  i-----
00:0a:5e:4b:4a:c0  3Com   intf  11  -57  i-----  public
00:0a:5e:4b:4a:c2  3Com   intf  11  -86  i-t1--  3Comwlan
00:0a:5e:4b:4a:c4  3Com   intf  11  -85  ic----  3com-ccmp
00:0a:5e:4b:4a:c6  3Com   intf  11  -85  i-t---  3com-tkip
00:0a:5e:4b:4a:c8  3Com   intf  11  -83  i----w  3com-voip
00:0a:5e:4b:4a:ca  3Com   intf  11  -85  i-----  3com-webaaa
...
```

Table 109 describes the fields in this display.

Table 109 display rfdetect visible Output

Field	Description
Transmit MAC	MAC address the rogue device that sent the 802.11 packet detected by the MAP radio.
Vendor	Company that manufactures or sells the rogue device.
Type	Classification of the rogue device: <ul style="list-style-type: none"> ■ rogue—Wireless device that is on the network but is not supposed to be on the network. ■ intf—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with MAP radios. ■ known—Device that is a legitimate member of the network.
Ch	Channel number on which the radio detected the rogue.

Table 109 display rfdetect visible Output (continued)

Field	Description
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal detected by the MAP radio, in decibels referred to 1 milliwatt (dBm).
Flags	Classification and encryption information for the rogue: <ul style="list-style-type: none"> ▪ The i, a, or u flag indicates the classification. ▪ The other flags indicate the encryption used by the rogue. For flag definitions, see the key in the command output.
SSID	SSID used by the detected device.

See Also

- **display rfdetect data** on page 642
- **display rfdetect mobility-domain** on page 644

set rfdetect active-scan

Disables or reenables active RF detection scanning on a WX switch. When active scanning is enabled, the MAP radios managed by the switch look for rogue devices by sending *probe any* requests (probe requests with a null SSID name), to solicit probe responses from other access points.

Syntax — `set rfdetect active-scan {enable | disable}`

- **enable** — Enables active RF detection scanning.
- **disable** — Disables active RF detection scanning.

Defaults — Active scanning is enabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You can enter this command on any WX switch in the Mobility Domain. The command takes effect only on that switch.

Examples — The following command disables active scanning on a WX switch:

```
WX1200# set rfdetect active-scan disable
success: off-channel scanning is disabled.
```

set rfdetect attack-list

Adds an entry to the attack list. The attack list specifies the MAC addresses of devices that MSS should issue countermeasures against whenever the devices are detected on the network. The attack list can contain the MAC addresses of APs and clients.

Syntax — `set rfdetect attack-list mac-addr`

- `mac-addr` — MAC address you want to attack.

Defaults — The attack list is empty by default.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — The attack list applies only to the WX switch on which the list is configured. WX switches do not share attack lists.

When on-demand countermeasures are enabled (with the **set radio-profile countermeasures configured** command) only those devices configured in the attack list are subject to countermeasures. In this case, devices found to be rogues by other means, such as policy violations or by determining that the device is providing connectivity to the wired network, are not attacked.

Examples — The following command adds MAC address aa:bb:cc:44:55:66 to the attack list:

```
WX4400# set rfdetect attack-list 11:22:33:44:55:66
success: MAC 11:22:33:44:55:66 is now in attacklist.
```

See Also

- **clear rfdetect attack-list** on page 630
- **display rfdetect attack-list** on page 635
- **set radio-profile countermeasures** on page 410

**set rfdetect
black-list**

Adds an entry to the client black list. The client black list specifies clients that are not allowed on the network. MSS drops all packets from the clients on the black list.

Syntax — `set rfdetect black-list mac-addr`

- `mac-addr` — MAC address you want to place on the black list.

Defaults — The client black list is empty by default.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — In addition to manually configured entries, the list can contain entries added by MSS. MSS can place a client in the black list due to an association, reassociation or disassociation flood from the client.

The client black list applies only to the WX switch on which the list is configured. WX switches do not share client black lists.

Examples — The following command adds client MAC address 11:22:33:44:55:66 to the black list:

```
WX1200# set rfdetect black-list 11:22:33:44:55:66
success: MAC 11:22:33:44:55:66 is now blacklisted.
```

See Also

- **display rfdetect black-list** on page 636
- **set rfdetect black-list** on page 654

**set rf detect
countermeasures**

Enables or disables countermeasures for the Mobility Domain. Countermeasures are packets sent by a radio to prevent clients from being able to use a rogue access point.



CAUTION: Countermeasures affect wireless service on a radio. When a MAP radio is sending countermeasures, the radio is disabled for use by network traffic, until the radio finishes sending the countermeasures.

Syntax — `set rfdetect countermeasures {enable | disable}`

- **enable** — Enables countermeasures.
- **disable** — Disables countermeasures.

Defaults — Countermeasures are disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command is valid only on the seed switch of the Mobility Domain.

Examples — The following command enables countermeasures for the Mobility Domain managed by this seed switch:

```
WX1200# set rfdetect countermeasures enable
success: countermeasures are now enabled.
```

See Also

- **clear rfdetect attack-list** on page 630
- **display rfdetect ignore** on page 644
- **set rfdetect countermeasures mac** on page 655

set rfdetect countermeasures mac

Starts countermeasures against a specific rogue.

Syntax — `set rfdetect countermeasures mac mac-addr`

- *mac-addr* — Basic service set identifier (BSSID) of the rogue. Enter the BSSID in MAC address format, using a colon between each octet (for example: aa:bb:cc:dd:ee:ff).

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Use this command to immediately begin countermeasures against a specific rogue in the rogue list. The MAC address you specify must be in the list of rogues generated by RF detection scans. MSS can issue countermeasures only against a device that is in the rogue list.

You can start countermeasures against more than one BSSID by typing additional **set rfdetect countermeasures mac** commands.



After you type the first **set rfdetect countermeasures mac** command, MSS does not issue countermeasures against any devices except the ones you specify using this command. To resume normal countermeasures operation, where MSS automatically issues countermeasures against detected rogues, use the **clear rfdetect countermeasures mac all** command.

This command is valid only on the seed switch of the Mobility Domain. The countermeasures take effect only if countermeasures are enabled for the Mobility Domain, using the **set rfdetect countermeasures enable** command.

This command does not become part of the configuration file when you save the configuration and therefore is not reloaded if the switch is restarted.

Examples — The following command begins countermeasures against rogue BSSID aa:bb:cc:11:22:33:

```
WX1200# set rfdetect countermeasures mac aa:bb:cc:11:22:33
success: set rfdetect countermeasures mac aa:bb:cc:11:22:33
```

See Also

- **clear rfdetect attack-list** on page 630
- **display rfdetect ignore** on page 644
- **set rf detect countermeasures** on page 654

set rfdetect ignore

Configures a list of known devices to ignore during an RF scan. MSS does not generate log messages or traps for the devices in the ignore list.

Syntax — **set rfdetect ignore mac-addr**

- *mac-addr* — BSSID (MAC address) of the device to ignore.

Defaults — MSS reports all unknown BSSIDs detected during an RF scan.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Use this command to identify third-party APs and other devices you are already aware of and do not want MSS to report following RF scans.

If you try to initiate countermeasures against a device on the ignore list, the ignore list takes precedence and MSS does not issue the countermeasures. Countermeasures apply only to rogue devices.

If you add a device that MSS has classified as a rogue to the permitted vendor list or permitted SSID list, but not to the ignore list, MSS can still classify the device as a rogue. Adding an entry to the permitted vendor list or permitted SSID list merely indicates that the device is from an allowed manufacturer or is using an allowed SSID. However, to cause MSS to stop classifying the device as a rogue, you must add the device's MAC address to the ignore list.

After you add a device that has been classified as a rogue to the ignore list, the device remains classified as a rogue for at least 10 minutes. After 10 minutes, MSS reclassifies the device as an interfering device.

Examples — The following command configures MSS to ignore BSSID `aa:bb:cc:11:22:33` during RF scans:

```
WX1200# set rfdetect ignore aa:bb:cc:11:22:33
success: MAC aa:bb:cc:11:22:33 is now ignored.
```

See Also

- **clear rfdetect ignore** on page 631
- **display rfdetect ignore** on page 644

set rfdetect log

Disables or reenables generation of log messages when rogues are detected or when they disappear.

Syntax — `set rfdetect log {enable | disable}`

- **enable** — Enables logging of rogues.
- **disable** — Disables logging of rogues.

Defaults — RF detection logging is enabled by default.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — This command is valid only on the seed switch of the Mobility Domain.

The log messages for rogues are generated only on the seed and appear only in the seed’s log message buffer. Use the **display log buffer** command to display the messages in the seed switch’s log message buffer.

Examples — The following command enables RF detection logging for the Mobility Domain managed by this seed switch:

```
WX1200# set rfdetect log enable
success: rfdetect logging is enabled.
```

See Also

- **display log buffer** on page 712

set rfdetect signature

Enables MAP signatures. A MAP signature is a set of bits in a management frame sent by a MAP that identifies that MAP to MSS. If someone attempts to spoof management packets from a 3Com MAP, MSS can detect the spoof attempt.

Syntax — `set rfdetect signature {enable | disable}`

- **enable** — Enables MAP signatures.
- **disable** — Disables MAP signatures.

Defaults — MAP signatures are disabled by default.

Access — Enabled.

History —Introduced in MSS Version 4.0.

Usage — The command applies only to MAPs managed by the WX switch on which you enter the command. To enable signatures on all MAPs in a Mobility Domain, enter the command on each WX switch in the Mobility Domain.



You must use the same MAP signature setting (enabled or disabled) on all WX switches in a Mobility Domain.

Examples — The following command enables MAP signatures on a WX switch:

```
WX1200# set rfdetect signature enable
success: signature is now enabled.
```

set rfdetect signature key

Creates an encrypted RF fingerprint key to use as a signature for a MAP.

Syntax — `set rfdetect signature key encrypted <key_value>`

- **key** — 16 bytes separated by colons generated by the user. For example, a1:b2:c3:d4:e5:f6:g7:h8 can be a key value.
- **encrypted** — Encrypts the signature key.

Defaults — Disabled by default.

Access — Enabled

History — Introduced in 5.0

set rfdetect ssid-list

Adds an SSID to the permitted SSID list. The permitted SSID list specifies the SSIDs that are allowed on the network. If MSS detects packets for an SSID that is not on the list, the AP that sent the packets is classified as a rogue. MSS issues countermeasures against the rogue if they are enabled.

Syntax — `set rfdetect ssid-list ssid-name`

- *ssid-name* — SSID name you want to add to the permitted SSID list.

Defaults — The permitted SSID list is empty by default and all SSIDs are allowed. However, after you add an entry to the list, MSS allows traffic only for the SSIDs that are on the list.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — The permitted SSID list applies only to the WX switch on which the list is configured. WX switches do not share permitted SSID lists.

If you add a device that MSS has classified as a rogue to the permitted SSID list, but not to the ignore list, MSS can still classify the device as a rogue. Adding an entry to the permitted SSID list merely indicates that the device is using an allowed SSID. However, to cause MSS to stop classifying the device as a rogue, you must add the device's MAC address to the ignore list.

Examples — The following command adds SSID *mycorp* to the list of permitted SSIDs:

```
WX1200# set rfdetect ssid-list mycorp
success:  ssid mycorp is now in ssid-list.
```

See Also

- **clear rfdetect ssid-list** on page 632
- **display rfdetect ssid-list** on page 649

set rfdetect vendor-list

Adds an entry to the permitted vendor list. The permitted vendor list specifies the third-party AP or client vendors that are allowed on the network. MSS does not list a device as a rogue or interfering device if the device's OUI is in the permitted vendor list.

Syntax — `set rfdetect vendor-list {client | ap} mac-addr`

- **client | ap** — Specifies whether the entry is for an AP brand or a client brand.
- **mac-addr** — Organizationally Unique Identifier (OUI) to remove.

Defaults — The permitted vendor list is empty by default and all vendors are allowed. However, after you add an entry to the list, MSS allows only the devices whose OUIs are on the list.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — The permitted vendor list applies only to the WX switch on which the list is configured. WX switches do not share permitted vendor lists.

If you add a device that MSS has classified as a rogue to the permitted vendor list, but not to the ignore list, MSS can still classify the device as a rogue. Adding an entry to the permitted vendor list merely indicates that the device is from an allowed vendor. However, to cause MSS to stop classifying the device as a rogue, you must add the device's MAC address to the ignore list.

Examples — The following command adds an entry for clients whose MAC addresses start with aa:bb:cc:

```
WX1200# set rfdetect vendor-list client aa:bb:cc:00:00:00
success: MAC aa:bb:cc:00:00:00 is now in client vendor-list.
```

The trailing 00:00:00 value is required.

See Also

- **clear rfdetect vendor-list** on page 633
- **display rfdetect vendor-list** on page 649

test rflink

Provides information about the RF link between the WX switch and the client based on sending test packets to the client.

Syntax — `test rflink {mac mac-addr | session-id session-id}`

- **mac-addr** — Tests the RF link between the WX switch and the client with the specified MAC address.
- **session-id** — Tests the RF link between the WX switch and the client with the specified local session ID.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — Use the **test rflink** command to send test packets to a specified client. The output of the command indicates the number of test packets received and acknowledged by the client, as well as the client's signal strength and signal-to-noise ratio.

Examples — The following command tests the RF link between the WX switch and the client with MAC address 00:0e:9b:bf:ad:13:

```
WX4400# test rflink mac 00:0e:9b:bf:ad:13
RF-Link Test to 00:0e:9b:bf:ad:13 :
Session-Id: 2
Packets Sent   Packets Rcvd   RSSI      SNR      RTT (micro-secs)
-----
                20             20       -68      26       976
```

Table 110 describes the fields in this display.

Table 110 test rflink Output

Field	Description
Packets Sent	The number of test packets sent from the WX switch to the client.
Packets Rcvd	The number of test packets acknowledged by the client.
RSSI	Received signal strength indication (RSSI)—the strength of the RF signal from the client, in decibels referred to 1 milliwatt (dBm).
SNR	Signal-to-noise ratio (SNR), in decibels (dB), of the data received from the client.
RTT (micro-secs)	The round-trip time, in microseconds, for the client response to the test packets.

See Also

- **display rfdetect data** on page 642
- **display rfdetect visible** on page 650

20

FILE MANAGEMENT COMMANDS

Use file management commands to manage system files and to display software and boot information.

Commands by Usage

This chapter presents file management commands alphabetically. Use Table 111 to locate commands in this chapter based on their use.

Table 111 File Management Commands by Usage

Type	Command
Software Version	reset system on page 683
	display version on page 677
Boot Settings	set boot partition on page 688
	set boot configuration-file on page 687
	set boot backup-configuration on page 686
	display boot on page 674
	clear boot config on page 666
	clear boot backup-configuration on page 666
File Management	dir on page 670
	copy on page 667
	md5 on page 681
	delete on page 669
	mkdir on page 681
	rmdir on page 685
Configuration File	save config on page 685
	load config on page 679
	display config on page 675

Table 111 File Management Commands by Usage (continued)

Type	Command
System Backup and Restore	backup on page 664
	restore on page 684
Sygate On-Demand Agent (SODA) file installation and removal	install soda agent on page 673
	display boot on page 674

backup

Creates an archive of WX system files and optionally, user file, in Unix *tape archive (tar)* format.

Syntax — `backup system [tftp:/ip-addr/]filename [all | critical]`

Defaults — All.

Access — Enabled.

History —.

Usage — You can create an archive located on a TFTP server or in the switch's nonvolatile storage. If you specify a TFTP server as part of the filename, the archive is copied directly to the TFTP server and not stored locally on the switch.

Use the **critical** option if you want to back up or restore only the system-critical files required to operate and communicate with the switch. Use the **all** option if you also want to back up or restore WebAAA pages, backup configuration files, image files, and any other files stored in the user files area of nonvolatile storage.

The maximum supported file size is 32 MB. If the file size of the tarball is too large, delete unnecessary files (such as unneeded copies of system image files) and try again, or use the **critical** option instead of the **all** option.

Neither option archives image files or any other files listed in the *Boot* section of **dir** command output. The **all** option archives image files only if they are present in the user files area.

Archive files created by the **all** option are larger than files created by the **critical** option. The file size depends on the files in the user area, and the file can be quite large if the user area contains image files.

The **backup** command places the boot configuration file into the archive. (The boot configuration file is the *Configured boot configuration* in the **display boot** command's output.) If the running configuration contains changes that have not been saved, these changes are not in the boot configuration file and are not archived. To make sure the archive contains the configuration that is currently running on the switch, use the **save config** command to save the running configuration to the boot configuration file, before using the **backup** command.

Examples — The following command creates an archive of the system-critical files and copies the archive directly to a TFTP server. The filename in this example includes a TFTP server IP address, so the archive is not stored locally on the switch.

```
WX1200# backup system tftp://10.10.20.9/sysa_bak critical
success: sent 28263 bytes in 0.324 seconds [ 87231 bytes/sec]
```

Table 112 describes the fields.

Table 112 Output for backup

Field	Description
[tftp://ip-addr/]filename	Name of the archive file to create. You can store the file locally in the switch's nonvolatile storage or on a TFTP server.
all	Backs up system files and all the files in the user files area. The user files area contains the set of files listed in the <i>file</i> section of dir command output.
critical	Backs up system files only, including the configuration file used when booting, and certificate files. The size of an archive created by this option is generally 1MB or less.

See Also

- **dir** on page 670
- **restore** on page 684

**clear boot
backup-configuration**

Clears the filename specified as the backup configuration file. In the event that MSS cannot read the configuration file at boot time, a backup configuration file is not used.

Syntax — `clear boot backup-configuration`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.1.

Examples — The following command clears the name specified as the backup configuration file from the configuration of the WX switch:

```
WX4400# clear boot backup-configuration
success: Backup boot config filename was cleared.
```

See Also

- **display boot** on page 674
- **set boot backup-configuration** on page 686

clear boot config

Resets to the factory default the configuration that MSS loads during a reboot.

Syntax — `clear boot config`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following commands back up the configuration file on a WX switch, reset the switch to its factory default configuration, and reboot the switch:

```
WX4400# copy configuration tftp://10.1.1.1/backupcfg
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
WX4400# clear boot config
success: Reset boot config to factory defaults.
```

```
WX4400# reset system force
..... rebooting .....
```

See Also

- **display config** on page 675
- **reset system** on page 683

copy

Performs the following copy operations:

- Copies a file from a TFTP server to nonvolatile storage.
- Copies a file from nonvolatile storage or temporary storage to a TFTP server.
- Copies a file from one area in nonvolatile storage to another.
- Copies a file to a new filename in nonvolatile storage.

Syntax — `copy source-url destination-url`

- *source-url* — Name and location of the file to copy. The uniform resource locator (URL) can be one of the following:
 - `[subdirname/]filename`
 - `file:[subdirname/]filename`
 - `tftp://ip-addr/[subdirname/]filename`
 - `tmp:filename`

For the filename, specify between 1 and 128 alphanumeric characters, with no spaces. Enter the IP address in dotted decimal notation.

The *subdirname/* option specifies a subdirectory.

- *destination-url* — Name of the copy and the location where to place the copy. The URL can be one of the following:
 - `[subdirname/]filename`
 - `file:[subdirname/]filename`
 - `tftp://ip-addr/[subdirname/]filename`

If you are copying a system image file into nonvolatile storage, the filename must include the boot partition name. You can specify one of the following:

- `boot0:/filename`
- `boot1:/filename`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The *filename* and **file:filename** URLs are equivalent. You can use either URL to refer to a file in an WX switch's nonvolatile memory. The **tftp://ip-addr/filename** URL refers to a file on a TFTP server. If DNS is configured on the WX switch, you can specify a TFTP server's hostname as an alternative to specifying the IP address.

The **tmp:filename** URL specifies a file in temporary storage. You can copy a file out of temporary storage but you cannot copy a file into temporary storage. Temporary storage is reserved for use by MSS.

If you are copying a system image file into nonvolatile storage, the filename must be preceded by the boot partition name, which can be **boot0** or **boot1**. Enter the filename as **boot0:/filename** or **boot1:/filename**. You must specify the boot partition that *was not* used to load the currently running image.

The maximum supported file size for TFTP is 32 MB.

Examples — The following command copies a file called *floorwx* from nonvolatile storage to a TFTP server:

```
WX4400# copy floorwx tftp://10.1.1.1/floorwx
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
```

The following command copies a file called *closetwx* from a TFTP server to nonvolatile storage:

```
WX4400# copy tftp://10.1.1.1/closetwx closetwx
success: received 637 bytes in 0.253 seconds [ 2517
bytes/sec]
```

The following command copies system image *WXA03001.Re1* from a TFTP server to boot partition 1 in nonvolatile storage:

```
WX4400# copy tftp://10.1.1.107/WXA03001.Re1
boot1:WXA03001.Re1
.....
.....success:
received 9163214 bytes in 105.939 seconds [ 86495 bytes/sec]
```

The following commands rename *test-config* to *new-config* by copying it from one name to the other in the same location, then deleting *test-config*:

```
WX4400# copy test-config new-config
WX4400# delete test-config
success: file deleted.
```

The following command copies file *corpa-login.html* from a TFTP server into subdirectory *corpa* in a WX switch's nonvolatile storage:

```
WX4400# copy tftp://10.1.1.1/corpa-login.html corpa/corpa-login.html
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
```

See Also

- **delete** on page 669
- **dir** on page 670

delete

Deletes a file.



CAUTION: *MSS does not prompt you to verify whether you want to delete a file. When you press Enter after typing a **delete** command, MSS immediately deletes the specified file.*



MSS does not allow you to delete the currently running software image file or the running configuration.

Syntax — `delete url`

- *url* — Filename. Specify between 1 and 128 alphanumeric characters, with no spaces.

If the file is in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example:

subdir_a/file_a.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You might want to copy the file to a TFTP server as a backup before deleting the file.

Examples — The following commands copy file *testconfig* to a TFTP server and delete the file from nonvolatile storage:

```
WX4400# copy testconfig tftp://10.1.1.1/testconfig
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
WX4400# delete testconfig
success: file deleted.
```

The following commands delete file *dang_doc* from subdirectory *dang*:

```
WX4400# delete dang/dang_doc
success: file deleted.
```

See Also

- **copy** on page 667
- **dir** on page 670

dir

Displays a list of the files in nonvolatile storage and temporary files.

Syntax — **dir** [*subdirname*] [**file:**] | [**core:**] | [**boot0:**] | [**boot1:**]

- *subdirname* — Subdirectory name. If you specify a subdirectory name, the command lists the files in that subdirectory. Otherwise, the command lists the files in the root directory and also lists the subdirectories.
- **file** — Limits **dir** output to the contents of the user files area.
- **core:** — Limits **dir** output to the contents of the */tmp/core* subdirectory.
- **boot0:** — Limits **dir** output to the contents of the *boot0* partition.
- **boot1:** — Limits **dir** output to the contents of the *boot1* partition

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. Core; file; boot0 and boot1 options added, to limit the output to the specified category, in MSS Version 4.0.

The following command limits the output to the contents of the user files area:

```
WX4400# dir file:
=====
file:
Filename                               Size                Created
file:configuration                     48 KB               Jul 12 2005, 15:02:32
file:corp2:corp2cnfig                  17 KB               Mar 14 2005, 22:20:04
corp_a/                                 512 bytes           May 21 2004, 19:15:48
file:dangcfg                            14 KB               Mar 14 2005, 22:20:04
dangdir/                                512 bytes           May 16 2004, 17:23:44
file:pubsconfig-april062005            40 KB               May 09 2005, 21:08:30
file:sysa_bak                           12 KB               Mar 15 2005, 19:18:44
file:testback                           28 KB               Apr 19 2005, 16:37:18
Total:                                159 Kbytes used, 207663 Kbytes free
```

The following command limits the output to the contents of the */tmp/core* subdirectory:

```
WX4400# dir core:
=====
file:
Filename                               Size                Created
core:command_audit.cur                 37 bytes            Aug 28 2005, 21:11:41
Total:                                37 bytes used, 91707 Kbytes free
```

The following command limits the output to the contents of the *boot0* partition:

```
WX4400# dir boot0:
=====
file:
Filename                               Size                Created
boot0:wx040100.020                     9780 KB             Aug 23 2005, 15:54:08
Total:                                9780 Kbytes used, 207663 Kbytes free
```

Table 113 describes the fields in the **dir** output.

Table 113 Output for dir

Field	Description
Filename	<p>Filename or subdirectory name.</p> <p>For files, the directory name is shown in front of the filename (for example, file:configuration). The <i>file:</i> directory is the root directory.</p> <p>For subdirectories, a forward slash is shown at the end of the subdirectory name (for example, old/).</p> <p>In the boot partitions list (Boot:), an asterisk (*) indicates the boot partition from which the currently running image was loaded and the image filename.</p>
Size	Size in Kbytes or bytes.
Created	System time and date when the file was created or copied onto the switch.
Total	Number of kilobytes in use to store files and the number that are still free.

See Also

- **copy** on page 667
- **delete** on page 669

install soda agent

Installs Sygate On-Demand (SODA) agent files in a directory on the WX switch.

Syntax — `install soda agent agent-file agent directory`
directory

- **agent-file** — Name of a .zip file on the WX switch containing SODA agent files.
- **directory** — Directory on the WX switch where SODA agent files are to be installed. The command automatically creates this directory.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — The install **soda agent command** installs a .zip file containing SODA agent files into a directory on the WX switch. Prior to installing the SODA agent files, you must have already copied the .zip file to the WX switch. This command creates the specified directory, unzips the file and places the contents into the directory. If the specified directory has the same name as a service profile, then that service profile uses the SODA agent files in the directory if SODA functionality is enabled for the service profile.

Examples — The following command installs the contents of the file *soda.ZIP* into a directory called *sp1*.

```
WX4400# install soda agent soda.ZIP agent-directory sp1
This command may take up to 20 seconds...
```

See Also

- **display boot** on page 674
- **set service-profile soda mode** on page 462

display boot

Displays the system image and configuration filenames used after the last reboot and configured for use after the next reboot.

Syntax — `display boot`

Defaults — None.

Access — Access.

History — Introduced in MSS Version 3.0. New fields, Configured boot version and Backup boot configuration added in MSS Version 4.0.

Examples — The following command shows the boot information for a WX switch:

```
WX1200# display boot
Configured boot version:          4.1.0.65
Configured boot image:           boot1:wx040100.020
Configured boot configuration:    file:configuration
Backup boot configuration:        file:backup.cfg
Booted version:                  4.1.0.65
Booted image:                    boot1:wx040100.020
Booted configuration:            file:configuration
Product model:                   WX
```

Table 114 describes the fields in the **display boot** output.

Table 114 Output for display boot

Field	Description
Configured boot version	Software version the switch will run next time the software is rebooted.
Configured boot image	Boot partition and image filename MSS will use to boot next time the software is rebooted.
Configured boot configuration	Configuration filename MSS will use to boot next time the software is rebooted.
Backup boot configuration	The name of the configuration file to be used in the event that MSS cannot read the configured boot configuration file next time the software is rebooted.
Booted version	Software version the switch is running.
Booted image	Boot partition and image filename MSS used the last time the software was rebooted. MSS is running this software image.
Booted configuration	Configuration filename MSS used to load the configuration the last time the software was rebooted.

See Also

- **display version** on page 677
- **reset system** on page 683
- **set boot configuration-file** on page 687

display config

Displays the configuration running on the WX.

Syntax — **display config** [**area** *area*] [*all*]

- **area** *area* — Configuration area. You can specify one of the following:
 - **aaa**
 - **acls**
 - **ap**
 - **arp**
 - **eapol**
 - **httpd**
 - **ip**

- `ip-config`
- `l2acl`
- `log`
- `mobility-domain`
- `network-domain`
- `ntp`
- `portconfig`
- `port-group`
- `qos`
- `radio-profile`
- `rfdetect`
- `service-profile`
- `sm`
- `snmp`
- `snoop`
- `spantree`
- `system`
- `trace`
- `vlan`
- `vlan-fdb`
- `vlan-profile`

If you do not specify a configuration area, nondefault information for all areas is displayed.

- `all` — Includes configuration items that are set to their default values.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. New options added for remote traffic monitoring (`snoop`) and `rfdevice` changed to `rfdetect` in MSS Version 4.0. Version 4.1 added new options `l2acl`, `network-domain`, and `qos`. Version 4.2 changed the `portgroup` to `port-group` for consistency with `clear port-group`, `set port-group`, and `display port-group` commands.

Usage — If you do not use one of the optional parameters, configuration commands that set nondefault values are displayed for all configuration areas. If you specify an area, commands are displayed for that area only. If you use the **all** option, the display also includes commands for configuration items that are set to their default values.

Examples — The following command shows configuration information for VLANs:

```
WX4400# display config area vlan
# Configuration nvgen'd at 2004-5-21 19:36:48
# Image 3.0.0
# Model WX4400
# Last change occurred at 2004-5-21 18:20:50
set vlan 1 port 1
```

See Also

- **load config** on page 679
- **save config** on page 685

display version

Displays software and hardware version information for an WX switch and, optionally, for any attached MAP access points.

Syntax — `display version [details]`

- **details** — Includes additional software build information and information about the MAP access points configured on the WX switch.

Defaults — None

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays version information for a WX switch:

```
WX1200# display version
```

```

Mobility System Software, Version: 4.1.0 QA 67
Copyright (c) 2002, 2003, 2004, 2005 3Com Corporation. All rights
reserved.
```

```

Build Information: (build#67) TOP 2005-07-21 04:41:00
Model:            WX
Hardware
  Mainboard:      version 24 ; revision 3 ; FPGA version 24
  PoE board:      version 1 ; FPGA version 6
Serial number     0321300013
Flash:            4.1.0.14 - md0a
Kernel:           3.0.0#20: Fri May 20 17:43:51 PDT 2005
BootLoader:       4.10 / 4.1.0
```

The following command displays additional software build information and MAP access point information:

```
WX1200# display version details
```

```

Mobility System Software, Version: 4.1.0 QA 67
Copyright (c) 2002, 2003, 2004, 2005 3Com Corporation. All rights
reserved.
```

```

Build Information: (build#67) TOP 2005-07-21 04:41:00
Label:            4.1.0.67_072105_WX20
Build Suffix:     -d-01
Model:            WX
Hardware
  Mainboard:      version 24 ; revision 3 ; FPGA version 24
  CPU Model:      750 (Revision 3.1)
  PoE board:      version 1 ; FPGA version 6
Serial number     0321300013
Flash:            4.1.0.14 - md0a
Kernel:           3.0.0#20: Fri May 20 17:43:51 PDT 2005
BootLoader:       4.10 / 4.1.0
```

Port/	AP	AP Model	Serial #	Versions
11	/-	MP-352	0424902948	H/W : A
				F/W1 : 5.6
				F/W2 : 5.6
				S/W : 4.1.0.67_072105_0432__AP
				BOOT S/W : 4.0.3.15_062705_0107__AP

Table 115 describes the fields in the **display version** output.

Table 115 Output for display version

Field	Description
Build Information	Factory timestamp of the image file.
Label	Software version and build date.
Build Suffix	Build suffix.
Model	Build model.
Hardware	Version information for the WX switch's motherboard and Power over Ethernet (PoE) board.
Serial number	Serial number of the WX switch.
Flash	Flash memory version.
Kernel	Kernel version.
BootLoader	Boot code version.
Port/AP	Port number connected to a MAP access point.
AP Model	MAP model number.
Serial #	MAP serial number.
Versions	MAP hardware, firmware, and software versions.

See Also

- **display boot** on page 674

load config

Loads configuration commands from a file and replaces the WX switch's running configuration with the commands in the loaded file.



CAUTION: *This command completely removes the running configuration and replaces it with the configuration contained in the file. 3Com recommends that you save a copy of the current running configuration to a backup configuration file before loading a new configuration.*

Syntax — **load config** [url]

- *url* — Filename. Specify between 1 and 128 alphanumeric characters, with no spaces.

If the file is in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example:

backup_configs/config_c.

Defaults — The default file location is nonvolatile storage.



The current version supports loading a configuration file only from the switch's nonvolatile storage. You cannot load a configuration file directly from a TFTP server.

If you do not specify a filename, MSS uses the same configuration filename that was used for the previous configuration load. For example, if the WX switch used *configuration* for the most recent configuration load, MSS uses *configuration* again unless you specify a different filename. To display the filename of the configuration file MSS loaded during the last reboot, use the **display boot** command.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command completely replaces the running configuration with the configuration in the file.

Examples — The following command reloads the configuration from the most recently loaded configuration file:

```
WX4400# load config
Reloading configuration may result in lost of connectivity,
do you wish to continue? (y/n) [n]y
success: Configuration reloaded
```

The following command loads configuration file *testconfig1*:

```
WX4400# load config testconfig1
Reloading configuration may result in lost of connectivity,
do you wish to continue? (y/n) [n]y
success: Configuration reloaded
```

See Also

- **display boot** on page 674
- **display config** on page 675
- **save config** on page 685

md5

Calculates the MD5 checksum for a file in the switch's nonvolatile storage.

Syntax — `md5 [boot0: | boot1:]filename`

- `boot0: | boot1:` — Boot partition into which you copied the file.
- `filename` — Name of the file.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — You must include the boot partition name in front of the filename. If you specify only the filename, the CLI displays a message stating that the file does not exist.

Examples — The following command calculates the checksum for image file WX040003.020 in boot partition 0:

```
pubs# md5 boot0:WX040003.020
MD5 (boot0:WX040003.020) = b9cf7f527f74608e50c70e8fb896392a
```

See Also

- **copy** on page 667
- **dir** on page 670

mkdir

Creates a new subdirectory in nonvolatile storage.

Syntax — `mkdir [subdirname]`

- `subdirname` — Subdirectory name. Specify between 1 and 32 alphanumeric characters, with no spaces.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following commands create a subdirectory called *corp2* and display the root directory to verify the result:

```
WX4400# mkdir corp2
success: change accepted.
WX4400# dir
=====
file:
Filename                               Size                Created
file:configuration                     17 KB               May 21 2004, 18:20:53
file:configuration.txt                 379 bytes          May 09 2004, 18:55:17
corp2/                                 512 bytes          May 21 2004, 19:22:09
corp_a/                                 512 bytes          May 21 2004, 19:15:48
file:dangcfg                            13 KB              May 16 2004, 18:30:44
dangdir/                                512 bytes          May 16 2004, 17:23:44
old/                                    512 bytes          Sep 23 2003, 21:58:48
Total:                                33 Kbytes used, 207822 Kbytes free
=====
Boot:
Filename                               Size                Created
*boot0:bload                           746 KB             May 09 2004, 19:02:16
*boot0:WXA03002.Rel                    8182 KB            May 09 2004, 18:58:16
boot1:WXA03001.Rel                      8197 KB            May 21 2004, 18:01:02
Boot0: Total:                          8928 Kbytes used, 3312 Kbytes free
Boot1: Total:                          8197 Kbytes used, 4060 Kbytes free
=====
temporary files:
Filename                               Size                Created
Total:                                0 bytes used, 93537 Kbytes free
```

See Also

- **dir** on page 670
- **rmdir** on page 685

reset system

Restarts an WX switch and reboots the software.

Syntax — `reset system [force]`

- **force** — Immediately restarts the system and reboots, without comparing the running configuration to the configuration file.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — If you do not use the **force** option, the command first compares the running configuration to the configuration file. If the running configuration and configuration file do not match, MSS does not restart the WX switch but instead displays a message advising you to either save the configuration changes or use the **force** option.

Examples — The following command restarts an WX switch that does not have any unsaved configuration changes:

```
WX4400# reset system  
This will reset the entire system. Are you sure (y/n)y
```

The following commands attempt to restart an WX switch with a running configuration that has unsaved changes, and then force the switch to restart:

```
WX4400# reset system  
error: Cannot reset, due to unsaved configuration changes.  
Use "reset system force" to override.  
WX4400# reset system force  
..... rebooting .....
```

See Also

- **display boot** on page 674
- **display version** on page 677
- **save config** on page 685

restore

Unzips a system archive created by the backup command and copies the files from the archive onto the switch.

Syntax `restore system [tftp://ip-addr/]filename [all | critical]`

Defaults — Critical.

Access — Enabled.

History — Introduced in MSS Version 3.2.

Usage — If a file in the archive has a counterpart on the switch, the archive version of the file replaces the file on the switch. The restore command does not delete files that do not have counterparts in the archive. For example, the command does not completely replace the user files area. Instead, files in the archive are added to the user files area. A file in the user area is replaced only if the archive contains a file with the same name.



Note: *If the archive's files cannot fit on the switch, the restore operation fails. 3Com recommends deleting unneeded image files before creating or restoring an archive.*

The **backup** command stores the MAC address of the switch in the archive. By default, the **restore** command works only if the MAC address in the archive matches the MAC address of the switch where the **restore** command is entered. The **force** option overrides this restriction and allows you to unpack one switch's archive onto another switch.



CAUTION: *Do not use the force option unless you are certain you want to replace the switch's files with files from another switch. If you restore one switch's system files onto another switch, you must generate new key pairs and certificates on the switch.*

Examples — The following command restores system-critical files on a switch, from archive sysa_bak.

```
WX1200# restore system tftp://10.10.20.9/sysa_bak
success: received 11908 bytes in 0.150 seconds [ 79386
bytes/sec]
success: restore complete.
```

See Also

- **backup** on page 664

rmdir

Removes a subdirectory from nonvolatile storage.

Syntax — **rmdir** [*subdirname*]

- *subdirname* — Subdirectory name. Specify between 1 and 32 alphanumeric characters, with no spaces.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — MSS does not allow the subdirectory to be removed unless it is empty. Delete all files from the subdirectory before attempting to remove it.

Examples — The following example removes subdirectory *corp2*:

```
WX4400# rmdir corp2
success: change accepted.
```

See Also

- **dir** on page 670
- **mkdir** on page 681

save config

Saves the running configuration to a configuration file.

Syntax — **save config** [*filename*]

- *filename* — Name of the configuration file. Specify between 1 and 128 alphanumeric characters, with no spaces.

To save the file in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example:

backup_configs/config_c.

Defaults — By default, MSS saves the running configuration as the configuration filename used during the last reboot.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — If you do not specify a filename, MSS replaces the configuration file loaded during the most recent reboot. To display the filename of the configuration file MSS loaded during the most recent reboot, use the **display boot** command.

The command completely replaces the specified configuration file with the running configuration.

Examples — The following command saves the running configuration to the configuration file loaded during the most recent reboot. In this example, the filename used during the most recent reboot is *configuration*.

```
WX4400# save config
Configuration saved to configuration.
```

The following command saves the running configuration to a file named *testconfig1*:

```
WX4400# save config testconfig1
Configuration saved to testconfig1.
```

See Also

- **display boot** on page 674
- **display config** on page 675
- **load config** on page 679

set boot backup-configuration

Specifies the name of a backup configuration file to be used in the event that MSS cannot read the WX switch's configuration file at boot time.

Syntax — `set boot backup-configuration filename`

- *filename* — Name of the file to use as a backup configuration file if MSS cannot read the WX switch's configuration file.

Defaults — By default, there is no backup configuration file.

Access — Enabled.

History —Introduced in MSS Version 4.1.

Examples — The following command specifies a file called backup.cfg as the backup configuration file on the WX switch:

```
WX1200# set boot backup-configuration backup.cfg
success: backup boot config filename set.
```

See Also

- **clear boot backup-configuration** on page 666
- **display boot** on page 674

set boot configuration-file

Changes the configuration file to load after rebooting.

Syntax — `set boot configuration-file filename`

- *filename* — Filename. Specify between 1 and 128 alphanumeric characters, with no spaces.

To load the file from a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example: **backup_configs/config_c**.

Defaults — The default configuration filename is *configuration*.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Usage — The file must be located in the switch's nonvolatile storage.

Examples — The following command sets the boot configuration file to *testconfig1*:

```
WX4400# set boot configuration-file testconfig1
success: boot config set.
```

set boot partition

Specifies the boot partition in which to look for the system image file following the next system reset, software reload, or power cycle.

Syntax — `set boot partition {boot0 | boot1}`

- `boot0` — Boot partition 0.
- `boot1` — Boot partition 1.

Defaults — By default, an WX switch uses the same boot partition for the next software reload that was used to boot the currently running image.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To determine the boot partition that was used to load the currently running software image, use the **dir** command.

Examples — The following command sets the boot partition for the next software reload to partition 1:

```
WX4400# set boot partition boot1
success: Boot partition set to boot1.
```

See Also

- **copy** on page 667
- **dir** on page 670
- **reset system** on page 683

uninstall soda agent

Removes the contents of a directory containing SODA agent files.

Syntax — `uninstall soda agent agent-directory directory`

- `directory` — Directory on the WX switch where soda agent files are to be removed.

Defaults — None.

Access — Enabled.

History — MSS Version 4.2.

Usage — The **uninstall soda command** removes the SODA agent directory and all of its contents. All files in the specified directory are removed. The command removes the directory and its contents, regardless of whether it contains SODA agent files.

Examples — The following command removes the directory *sp1* and all of its contents:

```
WX4400# uninstall soda agent agent-directory sp1  
This will delete all files in agent-directory, do you wish to  
continue? (y|n) [n]y
```

See Also

- **install soda agent** on page 673
- **set service-profile soda mode** on page 462

21

TRACE COMMANDS

Use trace commands to perform diagnostic routines. While MSS allows you to run many types of traces, this chapter describes commands for those traces you are most likely to use. For a complete listing of the types of traces MSS allows, type the **set trace ?** command.



CAUTION: Using the **set trace** command can have adverse effects on system performance. 3Com recommends that you use the lowest levels possible for initial trace commands, and slowly increase the levels to get the data you need.

Commands by Usage

This chapter presents trace commands alphabetically. Use Table 116 to locate commands in this chapter based on their use.

Table 116 Trace Commands by Usage

Type	Command
Trace	set trace sm on page 697
	set trace dot1x on page 696
	set trace authentication on page 694
	set trace authorization on page 695
	display trace on page 693
	save trace on page 694
	clear trace on page 692
	clear log trace on page 692

clear log trace

Deletes the log messages stored in the trace buffer.

Syntax — `clear log trace`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To delete the trace log, type the following command:

```
WX4400# clear log trace
```

See Also

- **display log buffer** on page 712
- **set log** on page 716

clear trace

Deletes running trace commands and ends trace processes.

Syntax — `clear trace {trace-area | all}`

- *trace-area* — Ends a particular trace process. Specify one of the following keywords to end the traces documented in this chapter:
 - **authorization** — Ends an authorization trace
 - **dot1x** — Ends an 802.1X trace
 - **authentication** — Ends an authentication trace
 - **sm** — Ends a session manager trace
- **all** — Ends all trace processes.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To clear all trace processes, type the following command:

```
WX4400# clear trace all
success: clear trace all
```

To clear the session manager trace, type the following command:

```
WX4400# clear trace sm
success: clear trace sm
```

See Also

- **display trace** on page 693
- **set trace authentication** on page 694
- **set trace authorization** on page 695
- **set trace dot1x** on page 696
- **set trace sm** on page 697

display trace

Displays information about traces that are currently configured on the WX switch, or all possible trace options.

Syntax — `display trace [all]`

- **all** — Displays all possible trace options and their configuration.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To view the traces currently running, type the following command:

```
WX4400# display trace
milliseconds spent printing traces: 1885.614
Trace Area          Level Mac          User          Port Filter
-----
dot1x                5                  0
sm                   5                  0
```

See Also

- **clear trace** on page 692
- **set trace authentication** on page 694
- **set trace authorization** on page 695
- **set trace dot1x** on page 696
- **set trace sm** on page 697

save trace

Saves the accumulated trace data for enabled traces to a file in the WX switch's nonvolatile storage.

Syntax — `save trace filename`

- *filename* — Name for the trace file. To save the file in a subdirectory, specify the subdirectory name, then a slash. For example: *traces/trace1*

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To save trace data into the file *trace1* in the subdirectory *traces*, type the following command:

```
WX4400# save trace traces/trace1
```

set trace authentication

Traces authentication information.

Syntax — `set trace authentication [mac-addr mac-address] [port port-num] [user username] [level level]`

- **mac-addr** *mac-address* — Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
- **port** *port-num* — Traces on a WX port number.
- **user** *username* — Traces a user. Specify a username of up to 32 alphanumeric characters with no spaces.
- **level** *level* — Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults — The default trace level is 5.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command starts a trace for information about user *jose*'s authentication:

```
WX4400# set trace authentication user jose
success: change accepted.
```

See Also

- **clear trace** on page 692
- **display trace** on page 693

set trace authorization

Traces authorization information.

Syntax — **set trace authorization** [**mac-addr** *mac-address*] [**port** *port-num*] [**user** *username*] [**level** *level*]

- **mac-addr** *mac-address* — Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
- **port** *port-num* — Traces on a WX a port number.
- **user** *username* — Traces a user. Specify a username of up to 80 alphanumeric characters with no spaces.
- **level** *level* — Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults — The default trace level is 5.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command starts a trace for information for authorization for MAC address 00:01:02:03:04:05:

```
WX4400# set trace authorization mac-addr 00:01:02:03:04:05
success: change accepted.
```

See Also

- **clear trace** on page 692
- **display trace** on page 693

set trace dot1x

Traces 802.1X sessions.

Syntax — `set trace dot1x [mac-addr mac-address] [port port-num]
[user username] [level level]`

- **mac-addr** *mac-address* — Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
- **port** *port-num* — Traces on a WX port number.
- **user** *username* — Traces a user. Specify a username of up to 80 alphanumeric characters with no spaces.
- **level** *level* — Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults — The default trace level is 5.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command starts a trace for the 802.1X sessions for MAC address 00:01:02:03:04:05:

```
WX4400# set trace dot1x mac-addr 00:01:02:03:04:05:
success: change accepted.
```

See Also

- **clear trace** on page 692
- **display trace** on page 693

set trace sm

Traces session manager activity.

Syntax — `set trace sm [mac-addr mac-address] [port port-num] [user username] [level level]`

- **mac-addr** *mac-address* — Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
- **port** *port-num* — Traces on a WX port number.
- **user** *username* — Traces a user. Specify a username of up to 80 alphanumeric characters, with no spaces.
- **level** *level* — Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults — The default trace level is 5.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — Type the following command to trace session manager activity for MAC address 00:01:02:03:04:05:

```
WX4400# set trace sm mac-addr 00:01:02:03:04:05:
success: change accepted.
```

See Also

- **clear trace** on page 692
- **display trace** on page 693

22

SNOOP COMMANDS

Use snoop commands to monitor wireless traffic, by using a MAP as a sniffing device. The MAP copies the sniffed 802.11 packets and sends the copies to an observer, which is typically a protocol analyzer such as Ethereal or Tethereal.

(For more information, including setup instructions for the monitoring station, see the “Remotely Monitoring Traffic” section in the “Troubleshooting a WX Switch” chapter of the [Wireless LAN Switch and Controller Configuration Guide](#).)

Commands by Usage

This chapter presents snoop commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Table 117 Remote Monitoring (Snooping) Commands By Usage

Remote monitoring (snooping)	set snoop on page 701
	display snoop info on page 706
	display snoop stats on page 708
	clear snoop on page 700
	set snoop map on page 704
	display snoop map on page 707
	display snoop on page 706
	clear snoop map on page 700
	set snoop mode on page 705
	display snoop stats on page 708

clear snoop

Deletes a snoop filter.

Syntax — `clear snoop filter-name`

- *filter-name* — Name of the snoop filter.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command deletes snoop filter *snoop1*:

```
WX1200# clear snoop snoop1
```

See Also

- **set snoop** on page 701
- **display snoop info** on page 706

clear snoop map

Removes a snoop filter from a MAP radio.

Syntax — `clear snoop map filter-name ap ap-num radio {1 | 2}`

- *filter-name* — Name of the snoop filter.
- `ap ap-num` — Number of a MAP to which the snoop filter is mapped.
- `radio 1` — Radio 1 of the MAP.
- `radio 2` — Radio 2 of the MAP. (This option does not apply to single-radio models.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command removes snoop filter *snoop2* from radio 2 on Distributed MAP 3:

```
WX1200# clear snoop map snoop2 ap 3 radio 2
success: change accepted.
```

The following command removes all snoop filter mappings from all radios:

```
WX1200# clear snoop map all
success: change accepted.
```

See Also

- **display snoop** on page 706
- **display snoop map** on page 707
- **set snoop map** on page 704

set snoop

Configures a snoop filter.

Syntax — **set snoop** *filter-name* [*condition-list*] [**observer** *ip-addr*] [**snap-length** *num*]

- *filter-name* — Name for the filter. The name can be up to 32 alphanumeric characters, with no spaces.
- *condition-list* — Match criteria for packets. Conditions in the list are ANDed. Therefore, to be copied and sent to an observer, a packet must match all criteria in the *condition-list*. You can specify up to eight of the following conditions in a filter, in any order or combination:
 - **frame-type** {*eq* | *neq*} {*beacon* | *control* | *data* | *management* | *probe*}
 - **channel** {*eq* | *neq*} *channel*
 - **bssid** {*eq* | *neq*} *bssid*
 - **src-mac** {*eq* | *neq*} *mac-addr*
 - **dest-mac** {*eq* | *neq*} *mac-addr*
 - **host-mac** {*eq* | *neq*} *mac-addr*
 - **mac-pair** *mac-addr1* *mac-addr2*
 - **direction** {*eq* | *neq*} {*transmit* | *receive*}

To match on packets to or from a specific MAC address, use the **dest-mac** or **src-mac** option. To match on both send and receive traffic for a host address, use the **host-mac** option. To match on a traffic flow (source and destination MAC addresses), use the **mac-pair** option. This option matches for either direction of a flow, and either MAC address can be the source or destination address.

If you omit a condition, all packets match that condition. For example, if you omit **frame-type**, all frame types match the filter.

For most conditions, you can use **eq** (equal) to match only on traffic that matches the condition value. Use **neq** (not equal) to match only on traffic that is not equal to the condition value.

- **observer** *ip-addr* — Specifies the IP address of the station where the protocol analyzer is located. If you do not specify an observer, the MAP radio still counts the packets that match the filter.
- **snap-length** *num* — Specifies the maximum number of bytes to capture. If you do not specify a length, the entire packet is copied and sent to the observer. 3Com recommends specifying a snap length of 100 bytes or less.

Defaults — No snoop filters are configured by default.

Access — Enabled.

History — Introduced in MSS Version 4.0. Version 6.0 added the direction filter.

Usage — Traffic that matches a snoop filter is copied after it is decrypted. The decrypted (clear) version is sent to the observer.

For best results:

- Do not specify an observer that is associated with the MAP where the snoop filter is running. This configuration causes an endless cycle of snoop traffic.
- If the snoop filter is running on a Distributed MAP, and the MAP used a DHCP server in its local subnet to configure its IP information, and the MAP did not receive a default gateway address as a result, the observer must also be in the same subnet. Without a default gateway, the MAP cannot find the observer.

- The MAP that is running a snoop filter forwards snooped packets directly to the observer. This is a one-way communication, from the MAP to the observer. If the observer is not present, the MAP still sends the snoop packets, which use bandwidth. If the observer is present but is not listening to TZSP traffic, the observer continuously sends ICMP error indications back to the MAP. These ICMP messages can affect network and MAP performance.

Examples — The following command configures a snoop filter named *snoop1* that matches on all traffic, and copies the traffic to the device that has IP address 10.10.30.2:

```
WX1200# set snoop snoop1 observer 10.10.30.2 snap-length 100
```

The following command configures a snoop filter named *snoop2* that matches on all data traffic between the device with MAC address aa:bb:cc:dd:ee:ff and the device with MAC address 11:22:33:44:55:66, and copies the traffic to the device that has IP address 10.10.30.3:

```
WX1200# set snoop snoop2 frame-type eq data mac-pair  
aa:bb:cc:dd:ee:ff 11:22:33:44:55:66 observer 10.10.30.3  
snap-length 100
```

See Also

- **clear snoop** on page 700
- **display snoop info** on page 706
- **display snoop stats** on page 708
- **set snoop map** on page 704
- **set snoop mode** on page 705

set snoop map

Maps a snoop filter to a radio on a MAP. A snoop filter does take effect until you map it to a radio and enable the filter.

Syntax — `set snoop map filter-name ap ap-num radio {1 | 2}`

- *filter-name* — Name of the snoop filter.
- `ap ap-num` — Number of a MAP to which to map the snoop filter.
- `radio 1` — Radio 1 of the MAP.
- `radio 2` — Radio 2 of the MAP. (This option does not apply to single-radio models.)

Defaults — Snoop filters are unmapped by default.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — You can map the same filter to more than one radio. You can map up to eight filters to the same radio. If more than one filter has the same observer, the MAP sends only one copy of a packet that matches a filter to the observer. After the first match, the MAP sends the packet and stops comparing the packet against other filters for the same observer.

If the filter does not have an observer, the MAP still maintains a counter of the number of packets that match the filter. (See **display snoop stats** on page 708.)

Examples — The following command maps snoop filter *snoop1* to radio 2 on MAP 3:

```
WX1200# set snoop map snoop1 ap 3 radio 2
success: change accepted.
```

See Also

- **clear snoop map** on page 700
- **display snoop map** on page 707
- **display snoop stats** on page 708
- **set snoop** on page 701
- **set snoop mode** on page 705

set snoop mode

Enables a snoop filter. A snoop filter does not take effect until you map it to a MAP radio and enable the filter.

Syntax — `set snoop {filter-name | all}`
`mode {enable [stop-after num-pkts] | disable}`

- *filter-name* | **all** — Name of the snoop filter. Specify **all** to enable all snoop filters.
- **enable** — Enables the snoop filter.
- **disable** — Disables the snoop filter.

Defaults — Snoop filters are disabled by default.

Access — Enabled.

History — Introduced in MSS Version 4.0. Version 6.0 removed the **stop-after** option. Also filter mode was made persistent across restarts.

Usage — The filter mode is retained even if you disable and reenables the radio, or restart the MAP or the WX switch. Once the filter is enabled, you must use the *disable* option to disable it.

Examples — The following command enables snoop filter *snoop1*:

```
WX# set snoop snoop1 mode enable
success: filter 'snoop1' enabled
```

See Also

- **display snoop** on page 706
- **display snoop info** on page 706
- **display snoop map** on page 707
- **display snoop stats** on page 708

display snoop

Displays the MAP radio mapping for all snoop filters.

Syntax — `display snoop`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — To display the mappings for a specific MAP radio, use the **display snoop map** command.

Examples — The following command shows the MAP radio mappings for all snoop filters configured on a WX switch:

```
WX1200# display snoop
ap: 3          Radio: 2
      snoop1
      snoop2
ap: 2          Radio: 2
      snoop2
```

See Also

- **clear snoop map** on page 700
- **display snoop map** on page 707
- **set snoop map** on page 704

display snoop info

Shows the configured snoop filters.

Syntax — `display snoop filter-name`

- *filter-name* — Name of the snoop filter.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command shows the snoop filters configured in the examples above:

```
WX1200# display snoop info
snoop1:
    observer 10.10.30.2 snap-length 100
    all packets
snoop2:
    observer 10.10.30.3 snap-length 100
    frame-type eq data
    mac-pair (aa:bb:cc:dd:ee:ff, 11:22:33:44:55:66)
```

See Also

- **clear snoop** on page 700
- **set snoop** on page 701

display snoop map

Shows the MAP radios that are mapped to a specific snoop filter.

Syntax — `display snoop map filter-name`

- *filter-name* — Name of the snoop filter.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — To display the mappings for all snoop filters, use the **display snoop** command.

Examples — The following command shows the mapping for snoop filter *snoop1*:

```
WX1200# display snoop map snoop1
filter 'snoop1' mapping
    ap: 3          Radio: 2
```

See Also

- **clear snoop map** on page 700
- **display snoop** on page 706
- **set snoop map** on page 704

display snoop stats Displays statistics for enabled snoop filters.

Syntax — `display snoop stats [filter-name [ap-num [radio {1 | 2}]]]`

- *filter-name* — Name of the snoop filter.
- *dap-num* — Number of a Distributed MAP to which the snoop filter is mapped
- **radio 1** — Radio 1 of the MAP
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — The MAP retains statistics for a snoop filter until the filter is changed or disabled. The MAP then clears the statistics.

Examples — The following command shows statistics for snoop filter *snoop1*:

```
WX1200# display snoop stats snoop1
Filter      ap Radio   Rx Match   Tx Match   Dropped   Stop-After
=====
snoop1      3          1          96         4 0       stopped
```

Table 118 describes the fields in this display.

Table 118 display snoop stats Output

Field	Description
Filter	Name of the snoop filter.
Dap	Distributed MAP containing the radio to which the filter is mapped.
Radio	Radio to which the filter is mapped.
Rx Match	Number of packets received by the radio that match the filter.
Tx Match	Number of packets sent by the radio that match the filter.
Dropped	Number of packets that matched the filter but that were not copied to the observer due to memory or network problems.
Stop-After	Filter state: <ul style="list-style-type: none"> ▪ running—enabled ▪ stopped—disabled ▪ <i>number-of-packets</i>—If the filter is running and the stop-after option was used to stop the filter, this field displays the number of packets that still need to match before the filter is stopped.

23

SYSTEM LOG COMMANDS

Use the system log commands to record information for monitoring and troubleshooting. MSS system logs are based on RFC 3164, which defines the log protocol.

Commands by Usage

This chapter present system log commands alphabetically. Use Table 119 to locate commands in this chapter based on their use.

Table 119 System Log Commands by Usage

Type	Command
System Logs	set log on page 716
	set log mark on page 719
	display log buffer on page 712
	display log config on page 714
	display log trace on page 715
	clear log on page 711

clear log

Clears the log messages stored in the log buffer, or removes the configuration for a syslog server and stops sending log messages to that server.

Syntax — `clear log [buffer | server ip-addr]`

- **buffer** — Deletes the log messages stored in nonvolatile storage.
- **server ip-addr** — Deletes the configuration for and stops sending log messages to the syslog server at this IP address. Specify an address in dotted decimal notation.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To stop sending system logging messages to a server at 192.168.253.11, type the following command:

```
WX4400# clear log server 192.168.253.11
success: change accepted.
```

Type the following command to clear all messages from the log buffer:

```
WX4400# clear log buffer
success: change accepted.
```

See Also

- **clear log trace** on page 692
- **set log** on page 716

display log buffer

Displays system information stored in the nonvolatile log buffer or the trace buffer.

Syntax — **display log buffer** [**{+|-}***number-of-messages*] [**facility** *facility-name*] [**matching** *string*] [**severity** *severity-level*]

- **buffer** — Displays the log messages in nonvolatile storage.
- **+|-** *number-of-messages* — Displays the number of messages specified as follows:
 - A positive number (for example, **+100**), displays that number of log entries starting from the oldest in the log.
 - A negative number (for example, **-100**) displays that number of log entries starting from newest in the log.
- **facility** *facility-name* — Area of MSS that is sending the log message. Type a space and a question mark (?) after **display log buffer facility** for a list of valid facilities.
- **matching** *string* — Displays messages that match a string—for example, a username or IP address.

- **severity** *severity-level* — Displays messages at a severity level greater than or equal to the level specified. Specify one of the following:
 - **emergency** — The WX switch is unusable.
 - **alert** — Action must be taken immediately.
 - **critical** — You must resolve the critical conditions. If the conditions are not resolved, the WX can reboot or shut down.
 - **error** — The WX is missing data or is unable to form a connection.
 - **warning** — A possible problem exists.
 - **notice** — Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required.
 - **info** — Informational messages only. No problem exists.
 - **debug** — Output from debugging.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The debug level produces a lot of messages, many of which can appear to be somewhat cryptic. Debug messages are used primarily by 3Com for troubleshooting and are not intended for administrator use.

Examples — Type the following command to see the facilities for which you can view event messages archived in the buffer:

```
WX4400# display log buffer facility ?
<facility name>          Select one of: KERNEL, AAA, SYSLOGD, ACL, APM, ARP,
ASO, BOOT, CLI, CLUSTER, COPP, CRYPTO, DOT1X, NET, ETHERNET, GATEWAY, HTTPD,
IGMP, IP, MISC, NOSE, NP, RAND, RESOLV, RIB, ROAM, ROGUE, SM, SNMPD, SPAN, STORE,
SYS, TAGMGR, TBRIDGE, TCPSSL, TELNET, TFTP, TLS, TUNNEL, VLAN, X509, XML, MAP,
RAPDA, WEBVIEW, EAP, FP, STAT, SSHD, SUP, DNSD, CONFIG, BACKUP.
```

The following command displays logged messages for the AAA facility:

```
WX4400# display log buffer facility AAA
AAA Jun. 25 09:11:32.579848 ERROR AAA_NOTIFY_ERR: AAA got SM
special event (98) on locality 3950 which is gone
```

See Also

- **clear log** on page 711
- **display log config** on page 714

display log config

Displays log configuration information.

Syntax — `display log config`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To display how logging is configured, type the following command:

```
WX4400# display log config
Logging console:                disabled
Logging console severity:      DEBUG
Logging sessions:              disabled
Logging sessions severity:     INFO
Logging buffer:                 enabled
Logging buffer severity:       DEBUG
Logging trace:                  enabled
Logging trace severity:        DEBUG
Logging buffer size:            10485760 bytes
Log marking:                    disabled
Log marking severity:          NOTICE
Log marking interval:           300 seconds

Logging server:                 172.21.12.19 port514 severity
                                EMERGENCY

Current session:                disabled
Current session severity:       INFO
```

See Also

- **clear log** on page 711
- **set log** on page 716

display log trace

Displays system information stored in the nonvolatile log buffer or the trace buffer.

Syntax — **display log trace** [**{+|-|/}***number-of-messages*]
[**facility** *facility-name*] [**matching** *string*]
[**severity** *severity-level*]

- **trace** — Displays the log messages in the trace buffer.
- **+|-|/number-of-messages** — Displays the number of messages specified as follows:
 - A positive number (for example, **+100**), displays that number of log entries starting from the oldest in the log.
 - A negative number (for example, **-100**) displays that number of log entries starting from newest in the log.
 - A number preceded by a slash (for example, **/100**) displays that number of the most recent log entries in the log, starting with the least recent.
- **facility** *facility-name* — Area of MSS that is sending the log message. Type a space and a question mark (**?**) after **display log trace facility** for a list of valid facilities.
- **matching** *string* — Displays messages that match a string—for example, a username or IP address.
- **severity** *severity-level* — Displays messages at a severity level greater than or equal to the level specified. Specify one of the following:
 - **emergency** — The WX switch is unusable.
 - **alert** — Action must be taken immediately.
 - **critical** — You must resolve the critical conditions. If the conditions are not resolved, the WX can reboot or shut down.
 - **error** — The WX is missing data or is unable to form a connection.
 - **warning** — A possible problem exists.
 - **notice** — Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required.
 - **info** — Informational messages only. No problem exists.
 - **debug** — Output from debugging.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — Type the following command to see the facilities for which you can view event messages archived in the buffer:

```
WX4400# display log trace facility ?
<facility name>          Select one of: KERNEL, AAA, SYSLOGD, ACL, APM, ARP,
ASO, BOOT, CLI, CLUSTER, COPP, CRYPTO, DOT1X, ENCAP, ETHERNET, GATEWAY, HTTPD,
IGMP, IP, MISC, NOSE, NP, RAND, RESOLV, RIB, ROAM, ROGUE, SM, SNMPD, SPAN, STORE,
SYS, TAGMGR, TBRIDGE, TCSSL, TELNET, TFTP, TLS, TUNNEL, VLAN, X509, XML, MAP,
RAPDA, WEBVIEW, EAP, PORTCONFIG, FP.
```

See Also

- **display log config** on page 714
- **clear log** on page 711

set log

Enables or disables logging of WX and MAP events to the WX log buffer or other logging destination and sets the level of the events logged. For logging to a syslog server only, you can also set the facility logged.

Syntax — **set log** {**buffer** | **console** | **current** | **sessions** | **trace**} [**severity** *severity-level*] **enable** | **disable**]

set log server *ip-addr* [**port** *port-number*]**severity** *severity-level* [**local-facility** *facility-level*]

- **buffer** — Sets log parameters for the log buffer in nonvolatile storage.
- **console** — Sets log parameters for console sessions.
- **current** — Sets log parameters for the current Telnet or console session. These settings are not stored in nonvolatile memory.
- **server** *ip-addr* — Sets log parameters for a syslog server. Specify an address in dotted decimal notation.
- **sessions** — Sets the default log values for Telnet sessions. You can set defaults for the following log parameters:
 - Severity

- Logging state (enabled or disabled)

To override the session defaults for an individual session, type the **set log** command from within the session and use the **current** option.

- **trace** — Sets log parameters for trace files.
- **port** *port-number* — Sets the TCP port for sending messages to the syslog server. You can specify a number from 1 to 65535. The default syslog port is 514.
- **severity** *severity-level* — Logs events at a severity level greater than or equal to the level specified. Specify one of the following:
 - **emergency** — The WX switch is unusable.
 - **alert** — Action must be taken immediately.
 - **critical** — You must resolve the critical conditions. If the conditions are not resolved, the WX can reboot or shut down.
 - **error** — The WX is missing data or is unable to form a connection.
 - **warning** — A possible problem exists.
 - **notice** — Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required.
 - **info** — Informational messages only. No problem exists.
 - **debug** — Output from debugging.
- **local-facility** *facility-level* — For messages sent to a syslog server, maps all messages of the severity you specify to one of the standard local log facilities defined in RFC 3164. You can specify one of the following values:
 - **0** — maps all messages to *local0*.
 - **1** — maps all messages to *local1*.
 - **2** — maps all messages to *local2*.
 - **3** — maps all messages to *local3*.
 - **4** — maps all messages to *local4*.
 - **5** — maps all messages to *local5*.
 - **6** — maps all messages to *local6*.
 - **7** — maps all messages to *local7*.

If you do not specify a local facility, MSS sends the messages with their default MSS facilities. For example, AAA messages are sent with facility 4 and boot messages are sent with facility 20 by default.

- **enable** — Enables messages to the specified target.
- **disable** — Disables messages to the specified target.

Defaults — The following are defaults for the **set log** commands.

- Events at the error level and higher are logged to the WX console.
- Events at the error level and higher are logged to the WX system buffer.
- Trace logging is enabled, and debug-level output is stored in the WX trace buffer.

Access — Enabled.

History — Introduced in MSS Version 3.0. Version 4.2 added the option **port**.

Usage — Using the command with only **enable** or **disable** turns logging on or off for the target at all levels. For example, entering **set log buffer enable** with no other keywords turns on logging to the system buffer of all facilities at all levels. Entering **set log buffer disable** with no other keywords turns off all logging to the buffer.

Examples — To log only emergency, alert, and critical system events to the console, type the following command:

```
WX4400# set log console severity critical enable
success: change accepted.
```

See Also

- **display log config** on page 714
- **clear log** on page 711

set log mark

Configures MSS to generate mark messages at regular intervals. The mark messages indicate the current system time and date. 3Com can use the mark messages to determine the approximate time when a system restart or other event causing a system outage occurred.

Syntax — `set log mark [enable | disable] [severity level] [interval interval]`

- **enable** — Enables the mark messages.
- **disable** — Disables the mark messages.
- **severity *level*** — Log severity at which the messages are logged:
 - emergency
 - alert
 - critical
 - error
 - warning
 - notice
 - info
 - debug
- **interval *interval*** — Interval at which MSS generates the mark messages. You can specify from 1 to 2147483647 seconds.

Defaults — Mark messages are disabled by default. When they are enabled, MSS generates a message at the notice level once every 300 seconds by default.

Access — Enabled.

History — Introduced in MSS Version 4.1.

Examples — The following command enables mark messages:

```
WX1200# set log mark enable
success: change accepted.
```

See Also

- **display log config** on page 714

24

BOOT PROMPT COMMANDS

Boot prompt commands enable you to perform basic tasks, including booting a system image file, from the boot prompt (boot>). A CLI session enters the boot prompt if MSS does not boot successfully or you intentionally interrupt the boot process. To interrupt the boot process, press **q** followed by **Enter** (return).



CAUTION: Generally, boot prompt commands are used only for troubleshooting. 3Com recommends that you use these commands only when working with 3Com Technical Support to diagnose a system issue. In particular, commands that change boot parameters can interfere with a WX switch's ability to boot successfully.

Boot Prompt Commands by Usage

This chapter presents boot prompt commands alphabetically. Use Table 120 to locate commands in this chapter based on their use.

Table 120 Boot Prompt Commands by Usage

Type	Command
Command Information	ls on page 734
	help on page 733
Booting	boot on page 723
	reset on page 736
	autoboot on page 722
	dhcp on page 728
File Management	dir on page 729
	fver on page 732
	version on page 738

Table 120 Boot Prompt Commands by Usage (continued)

Type	Command
Boot Profile Management	display on page 730
	create on page 726
Boot Profile Management, cont.	next on page 735
	change on page 725
	delete on page 727
Diagnostics	diag on page 729
	test on page 737

autoboot

Displays or changes the state of the autoboot option. The autoboot option controls whether a WX switch automatically boots a system image after initializing the hardware, following a system reset or power cycle.

Syntax — `autoboot [ON | on | OFF | off]`

- **ON** — Enables the autoboot option.
- **on** — Same effect as **ON**.
- **OFF** — Disables the autoboot option.
- **off** — Same effect as **OFF**.

Defaults — The autoboot option is enabled by default.

Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Examples — The following command displays the current setting of the autoboot option:

```
boot> autoboot
The autoboot flag is on.
```

See Also

- **boot** on page 723

boot

Loads and executes a system image file.

Syntax — `boot [BT=type] [DEV=device] [FN=filename]
[HA=ip-addr] [FL=num] [OPT=option] [OPT+=option]`

- **BT=*type*** — Boot type:
 - **c** — Compact flash. Boots using nonvolatile storage or a flash card.
 - **n** — Network. Boots using a TFTP server.
- **DEV=*device*** — Location of the system image file:
 - **c:** — Nonvolatile storage area containing boot partition 0
 - **d:** — Nonvolatile storage area containing boot partition 1
 - **e:** — Primary partition of the flash card in the flash card slot
 - **f:** — Secondary partition of the flash card in the flash card slot
 - **boot0** — boot partition 0
 - **boot1** — boot partition 1
- **FN=*filename*** — System image filename.
- **HA=*ip-addr*** — Host address (IP address) of a TFTP server. This parameter applies only when the boot type is **n** (network).
- **FL=*num*** — Number representing the bit settings of boot flags to pass to the booted system image. Use this parameter only if advised to do so by 3Com.
- **OPT=*option*** — String up to 128 bytes of boot options to pass to the booted system image *instead of* the boot option(s) in the currently active boot profile. The options temporarily replace the options in the boot profile. Use this parameter only if advised to do so by 3Com.
- **OPT+=*option*** — String up to 128 bytes of boot options to pass to the booted system image *in addition to* the boot option(s) in the currently active boot profile. The options are appended to the options already in the boot profile. Use this parameter only if advised to do so by 3Com.

Defaults — The boot settings in the currently active boot profile are used by default.

Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Usage — If you use an optional parameter, the parameter setting overrides the setting of the same parameter in the currently active boot profile. However, the boot profile itself is not changed. To display the currently active boot profile, use the **display** command. To change the currently active boot profile, use the **change** command.

Examples — The following command loads system image file WXA30001.Rel from boot partition 1:

```
boot> boot FN=WXA03001.Rel DEV=boot1
Compact Flash load from boot0:WXA03001.Rel.
unzip: Inflating ramdisk_3.0.1_092304_WX4400 OK
unzip file len 36196930 OK
```

```
Copyright (c) 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004
```

```
The NetBSD Foundation, Inc. All rights reserved.
```

```
Copyright (c) 1982, 1986, 1989, 1991, 1993
```

```
The Regents of the University of California. All rights reserved.
```

```
Detecting hardware...done.
```

```
readclock: 2004-9-29 21:45:7.31 UTC
```

```
system initialized (3.0.1), starting MSS
```

```
Executing update_3
```

```
Starting supervisor 3.0.1_092304_WX4400 ...
```

```
SNMPD Sep 29 21:45:34.262293 NOTICE SNMPD: SNMP Agent Resident Module Version
16.1.0.0
```

```
SNMPD Sep 29 21:45:34.263146 NOTICE SNMPD: Copyright (c) 2004 3Com Corporation.
All rights reserved.
```

```
SYS Sep 29 21:45:36.849457 NOTICE Port 1 up 1000 Full Duplex
```

```
SYSLOGD Sep 29 21:45:38.857125 ALERT SYSTEM_READY: The system has finished
booting. (cause was "Warm Reboot")
```

```
Copyright (c) 2004 3Com Corporation. All rights reserved.
```

```
Username:
```

See Also

- **change** on page 725
- **display** on page 730

change

Changes parameters in the currently active boot profile. (For information about boot profiles, see **display** on page 730.)

Syntax — `change`

Defaults — The default boot type is **c** (compact flash). The default filename is *default*. The default flags setting is 0x00000000 (all flags disabled) and the default options list is `run=nos;boot=0`. The default device setting is the boot partition specified by the most recent **set boot partition** command typed at the Enabled level of the CLI, or boot 0 if the command has never been typed.

Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Usage — After you type the **change** command, the system interactively displays the current setting of each parameter and prompts you for the new setting. When prompted, type the new setting, press Enter to accept the current setting, or type . (period) to change the setting to its default value. To back up to the previous parameter, type - (hyphen).

For information about each of the boot parameters you can set, see **display** on page 730.

Examples — The following command enters the configuration mode for the currently active boot profile, changes the device to **boot1**, and leaves the other parameters with their current settings:

```
boot> change
Changing the default configuration is not recommended.
Are you sure that you want to proceed? (y/n)

BOOT TYPE:      [c]
DEVICE:         [boot0:]boot1
FILENAME:       [default]
FLAGS:          [0x00000000]
OPTIONS:        [run=nos;boot=0]
```

The following command enters the configuration mode for the currently active boot profile and configures the WX switch (in this example, an WXR100) to boot using a TFTP server:

```
boot> change
Changing the default configuration is not recommended.
Are you sure that you want to proceed? (y/n)y

BOOT TYPE:      [c]> n
DEVICE:         [boot0:]> emac1
FILENAME:       [default]> bootfile
HOST IP:        [0.0.0.0]> 172.16.0.1
LOCAL IP:       [0.0.0.0]> 172.16.0.21
GATEWAY IP:     [0.0.0.0]> 172.16.0.20
IP MASK:        [0.0.0.0]> 255.255.255.0
FLAGS:         [0x00000000]>
OPTIONS:        [run=nos;boot=0]>
```

See Also

- **boot** on page 723
- **create** on page 726
- **delete** on page 727
- **dhcp** on page 728
- **display** on page 730
- **next** on page 735

create

Creates a new boot profile. (For information about boot profiles, see **display** on page 730.)

Syntax — **create**

Defaults — The new boot profile has the same settings as the currently active boot profile by default.

Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Usage — A WX switch can have up to four boot profiles. The boot profiles are stored in slots, numbered 0 through 3. When you create a new profile, the system uses the next available slot for the profile. If all four slots already contain profiles and you try to create a fifth profile, the switch displays a message advising you to change one of the existing profiles instead.

To make a new boot profile the currently active boot profile, use the **next** command. To change boot parameter settings, use the **change** command.

Examples — The following command creates a new boot profile in slot 1 on a WX switch that currently has only one boot profile, in slot 0:

```
boot> create

      BOOT Index:    1
      BOOT TYPE:     c
      DEVICE:        boot1:
      FILENAME:      default
      FLAGS:         00000000
      OPTIONS:       run=nos;boot=0
```

See Also

- **change** on page 725
- **delete** on page 727
- **display** on page 730
- **next** on page 735

delete

Removes the currently active boot profile. (For information about boot profiles, see **display** on page 730.)

Syntax — `delete`

Defaults — None.

Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Usage — When you type the **delete** command, the next-lower numbered boot profile becomes the active profile. For example, if the currently active profile is number 3, profile number 2 becomes active after you type **delete** to delete profile 3. You cannot delete boot profile 0.

Examples — To remove the currently active boot profile, type the following command:

```
boot> delete

      BOOT Index:    1
      BOOT TYPE:     c
      DEVICE:        boot1:
      FILENAME:      default
      FLAGS:         00000000
      OPTIONS:       run=nos;boot=0
```

See Also

- **change** on page 725
- **create** on page 726
- **display** on page 730
- **next** on page 735

dhcp

Displays or changes the state of the DHCP option. The DHCP option controls whether a WX switch uses DHCP to obtain its IP address when it is booted using a TFTP server.

Syntax — `dhcp [ON | on | OFF | off]`

- **ON** — Enables the DHCP option.
- **on** — Same effect as **ON**.
- **OFF** — Disables the DHCP option.
- **off** — Same effect as **OFF**.

Defaults — The DHCP option is disabled by default.

Access — Boot prompt.

History — Introduced in MSS Version 1.0.

Examples — The following command displays the current setting of the DHCP option:

```
boot> dhcp
DHCP is currently enabled.
```

The following command disables the DHCP option:

```
boot> dhcp
DHCP is currently disabled.
```

See Also

- **boot** on page 723

diag

Accesses the diagnostic mode.

Syntax — `diag`

Defaults — The diagnostic mode is disabled by default.

Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Usage — Access to the diagnostic mode requires a password, which is not user configurable. Use this mode only if advised to do so by 3Com.

dir

Displays the boot code and system image files on a WX switch.

Syntax — `dir [c: | d: | e: | f: | boot0 | boot1]`

- **c:** — Nonvolatile storage area containing boot partition 0 (primary).
- **d:** — Nonvolatile storage area containing boot partition 1 (secondary).
- **e:** — Primary partition of the flash card in the flash card slot.
- **f:** — Secondary partition of the flash card in the flash card slot.
- **boot0** — Boot partition 0.
- **boot1** — Boot partition 1.

Defaults — None.

Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Usage — To display the system image software versions, use the **fver** command. This command does not list the boot code versions. To display the boot code versions, use the **version** command.

Examples — The following command displays all the boot code and system image files on a WX switch:

```
boot> dir
```

```
Internal Compact Flash Directory (Primary):
      WXA30001.Rel                8863722 bytes

      Internal Compact Flash Directory (Secondary):
      WXA30001.Rel                8862885 bytes
```

See Also

- **fver** on page 732
- **version** on page 738

display

Displays the currently active boot profile. A boot profile is a set of parameters that a WX switch uses to control the boot process. Each boot profile contains the following parameters:

- **Boot type** — Either compact flash (local device on the WX switch) or network (TFTP)
- **Boot device** — Location of the system image file
- **Filename** — System image file
- **Flags** — Number representing the bit settings of boot flags to pass to the booted system image.
- **Options** — String up to 128 bytes of boot options to pass to the booted system image

A WX switch can have up to four boot profiles, numbered 0 through 3. Only one boot profile can be active at a time. You can create, change, and delete boot profiles. You also can activate another boot profile in place of the currently active one.

Syntax — `display`

Defaults — None.

Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Examples — To display the currently active boot profile, type the following command at the boot prompt:

```
boot> display

BOOT Index:    0
BOOT TYPE:    c
DEVICE:        boot1:
FILENAME:      default
FLAGS:         00000000
OPTIONS:       run=nos;boot=0
```

Table 121 describes the fields in the display.

Table 121 Output of display command

Field	Description
BOOT Index	Boot profile slot, which can be a number from 0 to 3.
BOOT TYPE	Boot type: <ul style="list-style-type: none"> ▪ c — Compact flash. Boots using nonvolatile storage or a flash card. ▪ n — Network. Boots using a TFTP server.

Table 121 Output of display command (continued)

Field	Description
DEVICE	Location of the system image file: <ul style="list-style-type: none"> ▪ c: — Nonvolatile storage area containing boot partition 0 ▪ d: — Nonvolatile storage area containing boot partition 1 ▪ e: — Primary partition of the flash card in the flash card slot ▪ f: — Secondary partition of the flash card in the flash card slot ▪ boot0 — boot partition 0 ▪ boot1 — boot partition 1
FILENAME	System image file name.
FLAGS	Number representing the bit settings of boot flags to pass to the booted system image.
OPTIONS	String up to 128 bytes of boot options to pass to the booted system image.

See Also

- **change** on page 725
- **create** on page 726
- **delete** on page 727
- **next** on page 735

fver

Displays the version of a system image file installed in a specific location on a WX switch.

Syntax — **fver** {**c:** | **d:** | **e:** | **f:** | **boot0:** | **boot1:**}
[filename]

- **c:** — Nonvolatile storage area containing boot partition 0 (primary).
- **d:** — Nonvolatile storage area containing boot partition 1 (secondary).
- **e:** — Primary partition of the flash card in the flash card slot.
- **f:** — Secondary partition of the flash card in the flash card slot.
- **boot0:** — Boot partition 0.
- **boot1:** — Boot partition 1.
- *filename* — System image filename.

Defaults — None.

Access — Boot prompt.

History —Introduced in MSS Version 3.0.

Usage — To display the image filenames, use the **dir** command. This command does not list the boot code versions. To display the boot code versions, use the **version** command.

Examples — The following command displays the system image version installed in boot partition 1:

```
boot> fver boot1
File boot1:default version is 3.0.1.
```

See Also

- **dir** on page 729
- **version** on page 738

help

Displays a list of all the boot prompt commands or detailed information for an individual command.

Syntax — **help** [*command-name*]

- *command-name* — Boot prompt command.

Defaults — None.

Access — Boot prompt.

History —Introduced in MSS Version 3.0.

Usage — If you specify a command name, detailed information is displayed for that command. If you do not specify a command name, all the boot prompt commands are listed.

Examples — The following command displays detailed information for the **fver** command:

```
boot> help fver
```

```
fver Display the version of the specified device:filename.
```

```
USAGE: fver [c:file|d:file|e:file|f:file|boot0:file|boot1:file|
boot2:file|boot3:file]
```

Command to display the version of the compressed image file associated with the given device:filename.

See Also

- **ls** on page 734

ls

Displays a list of the boot prompt commands.

Syntax — **ls**

Defaults — None.

Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Usage — To display help for an individual command, type help followed by the command name (for example, **help boot**).

Examples — To display a list of the commands available at the boot prompt, type the following command:

```
boot> ls
  ls      Display a list of all commands and descriptions.
  help    Display help information for each command.
  autoboot Display the state of, enable, or disable the autoboot option.
  boot    Load and execute an image using the current boot configuration
profile.
  change  Change the current boot configuration profile.
  create  Create a new boot configuration profile.
  delete  Delete the current boot configuration profile.
  next    Select the next boot configuration profile.
  display Display the current boot configuration profile.

  dir     Display the contents of the specified boot partition.
  fver    Display the version of the loadable image specified by
device:filename.
  version Display HW and Bootstrap/Bootloader version information.
  reset   Reset the system.
  test    Display the state of, enable, or disable the tests option.
  diag    Access the diagnostic command CLI.
```

See Also

- **help** on page 733

next

Activates and displays the boot profile in the next boot profile slot. (For information about boot profiles, see **display** on page 730.)

Syntax — `next`

Defaults — None.

Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Usage — A WX switch contains 4 boot profile slots, numbered 0 through 3. This command activates the boot profile in the next slot, in ascending numerical order. If the currently active slot is 3, the command activates the boot profile in slot 0.

Examples — To activate the boot profile in the next slot and display the profile, type the following command:

```
boot> next

      BOOT Index:    0
      BOOT TYPE:     c
      DEVICE:        boot1:
      FILENAME:      testcfg
      FLAGS:         00000000
      OPTIONS:       run=nos;boot=0
```

See Also

- **change** on page 725
- **create** on page 726
- **delete** on page 727
- **display** on page 730

reset

Resets a WX switch's hardware.

Syntax — `reset`

Defaults — None.

Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Usage — After resetting the hardware, the **reset** command attempts to load a system image file only if other boot settings are configured to do so.

Examples — To immediately reset the system, type the following command at the boot prompt:

```
boot> reset

WX Bootstrap 3.1 Release
Testing Low Memory 1 .....
Testing Low Memory 2 .....
CISTPL_VERS_1:  4.1  <SanDisk> <SDP> <5/3 0.6>
Reset Cause (0x0100) is WARM
```



```

3Com WX-4400 Bootstrap/Bootloader

                          Version 3.0.2 Release
Compiled on Wed Sep 22 09:18:47 PDT 2004 by

  Bootstrap 0 version:      3.1      Active
  Bootloader 0 version:    3.0.2     Active
  Bootstrap 1 version:      3.1
  Bootloader 1 version:    3.0.1

      WX-4400 Board Revision: 2.
WX-4400 Controller Revision: 5.
      WXA30001.Rel           8863722 bytes

  BOOT Index: 0
  BOOT TYPE:  c
  DEVICE:     boot0:
  FILENAME:   default
  FLAGS:      00000000
  OPTIONS:    run=nos;root=md0a

```

See Also

- **boot** on page 723

test

Displays or changes the state of the poweron test flag. The poweron test flag controls whether a WX performs a set of self tests prior to the boot process.

Syntax — `test [ON | on | OFF | off]`

- **ON** — Enables the poweron test flag.
- **on** — Same effect as **ON**.
- **OFF** — Disables the poweron test flag.
- **off** — Same effect as **OFF**.

Defaults — The poweron test flag is disabled by default.

Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Examples — The following command displays the current setting of the poweron test flag:

```
boot> test
The diagnostic execution flag is not set.
```

See Also

- **boot** on page 723

version

Displays version information for a WX switch's hardware and boot code.

Syntax — `version`

Defaults — None.

Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Usage — This command does not list the system image file versions installed in the boot partitions. To display system image file versions, use the **dir** or **fver** command.

Examples — To display hardware and boot code version information, type the following command at the boot prompt:

```
boot> version

3Com WX-4400 Bootstrap/Bootloader

                Version 3.0.2 Release
Compiled on Wed Sep 22 09:18:47 PDT 2004 by

  Bootstrap 0 version:           3.1      Active
  Bootloader 0 version:         3.0.2    Active
  Bootstrap 1 version:           3.1
  Bootloader 1 version:         3.0.1

      WX-4400 Board Revision:     2.
  WX-4400 Controller Revision:   5.
```

See Also

- **dir** on page 729
- **fver** on page 732

A

OBTAINING SUPPORT FOR YOUR 3COM PRODUCTS

3Com offers product registration, case management, and repair services through eSupport.3com.com. You must have a user name and password to access these services, which are described in this appendix.

Register Your Product to Gain Service Benefits

To take advantage of warranty and other service benefits, you must first register your product at:

<http://eSupport.3com.com/>

3Com eSupport services are based on accounts that are created or that you are authorized to access.

Solve Problems Online

3Com offers the following support tool:

- **3Com Knowledgebase** — Helps you to troubleshoot 3Com products. This query-based interactive tool is located at:

<http://knowledgebase.3com.com>

It contains thousands of technical solutions written by 3Com support engineers.

Purchase Extended Warranty and Professional Services

To enhance response times or extend your warranty benefits, you can purchase value-added services such as 24x7 telephone technical support, software upgrades, onsite assistance, or advanced hardware replacement.

Experienced engineers are available to manage your installation with minimal disruption to your network. Expert assessment and implementation services are offered to fill resource gaps and ensure the success of your networking projects. For more information on 3Com Extended Warranty and Professional Services, see:

<http://www.3com.com/>

Contact your authorized 3Com reseller or 3Com for additional product and support information. See the table of access numbers later in this appendix.

Access Software Downloads

You are entitled to *bug fix / maintenance releases* for the version of software that you initially purchased with your 3Com product. To obtain access to this software, you need to register your product and then use the Serial Number as your login. Restricted Software is available at:

<http://eSupport.3com.com/>

To obtain software releases that *follow* the software version that you originally purchased, 3Com recommends that you buy an Express or Guardian contract, a Software Upgrades contract, or an equivalent support contract from 3Com or your reseller. Support contracts that include software upgrades cover feature enhancements, incremental functionality, and bug fixes, but they do not include software that is released by 3Com as a separately ordered product. Separately orderable software releases and licenses are listed in the 3Com Price List and are available for purchase from your 3Com reseller.

Contact Us

3Com offers telephone, internet, and e-mail access to technical support and repair services. To access these services for your region, use the appropriate telephone number, URL, or e-mail address from the table in the next section.

Telephone Technical Support and Repair

To obtain telephone support as part of your warranty and other service benefits, you must first register your product at:

<http://eSupport.3com.com/>

When you contact 3Com for assistance, please have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision level
- Diagnostic error messages
- Details about recent configuration changes, if applicable

To send a product directly to 3Com for repair, you must first obtain a return materials authorization number (RMA). Products sent to 3Com without authorization numbers clearly marked on the outside of the package will be returned to the sender unopened, at the sender's expense. If your product is registered and under warranty, you can obtain an RMA number online at <http://eSupport.3com.com/>. First-time users must apply for a user name and password.

Telephone numbers are correct at the time of publication. Find a current directory of 3Com resources by region at:

<http://csoweb4.3com.com/contactus/>

Country	Telephone Number	Country	Telephone Number
Asia, Pacific Rim — Telephone Technical Support and Repair			
Australia	1800 075 316	Philippines	1800 144 10220 or 029003078
Hong Kong	2907 0456	PR of China	800 810 0504
India	000 800 440 1193	Singapore	800 616 1463
Indonesia	001 803 852 9825	South. Korea	080 698 0880
Japan	03 3507 5984	Taiwan	00801 444 318
Malaysia	1800 812 612	Thailand	001 800 441 2152
New Zealand	0800 450 454		

Country	Telephone Number	Country	Telephone Number
Pakistan	Call the U.S. direct by dialing 00 800 01001, then dialing 800 763 6780		
Sri Lanka	Call the U.S. direct by dialing 02 430 430, then dialing 800 763 6780		
Vietnam	Call the U.S. direct by dialing 1 201 0288, then dialing 800 763 6780		

You can also obtain non-urgent support in this region at this email address ap_r technical_support@3com.com
 Or request a return material authorization number (RMA) by FAX using this number: +61 2 9937 5048, or send an email at this email address: ap_rma_request@3com.com

Europe, Middle East, and Africa — Telephone Technical Support and Repair

From anywhere in these regions not listed below, call: +44 1442 435529

From the following countries, call the appropriate number:

Austria	0800 297 468	Luxembourg	800 23625
Belgium	0800 71429	Netherlands	0800 0227788
Denmark	800 17309	Norway	800 11376
Finland	0800 113153	Poland	00800 4411 357
France	0800 917959	Portugal	800 831416
Germany	0800 182 1502	South Africa	0800 995 014
Hungary	06800 12813	Spain	900 938 919
Ireland	1 800 553 117	Sweden	020 795 482
Israel	180 945 3794	Switzerland	0800 553 072
Italy	800 879489	U.K.	0800 096 3266

You can also obtain support in this region using this URL: <http://emea.3com.com/support/email.html>

You can also obtain non-urgent support in this region at these email addresses:

Technical support and general requests: customer_support@3com.com

Return material authorization: warranty_repair@3com.com

Contract requests: emea_contract@3com.com

Latin America — Telephone Technical Support and Repair

Antigua	1 800 988 2112	Guatemala	AT&T +800 998 2112
Argentina	0 810 444 3COM	Haiti	57 1 657 0888
Aruba	1 800 998 2112	Honduras	AT&T +800 998 2112
Bahamas	1 800 998 2112	Jamaica	1 800 998 2112
Barbados	1 800 998 2112	Martinique	571 657 0888
Belize	52 5 201 0010	Mexico	01 800 849CARE
Bermuda	1 800 998 2112	Nicaragua	AT&T +800 998 2112
Bonaire	1 800 998 2112	Panama	AT&T +800 998 2112
Brazil	0800 13 3COM	Paraguay	54 11 4894 1888
Cayman	1 800 998 2112	Peru	AT&T +800 998 2112
Chile	AT&T +800 998 2112	Puerto Rico	1 800 998 2112
Colombia	AT&T +800 998 2112	Salvador	AT&T +800 998 2112
Costa Rica	AT&T +800 998 2112	Trinidad and Tobago	1 800 998 2112
Curacao	1 800 998 2112	Uruguay	AT&T +800 998 2112
Ecuador	AT&T +800 998 2112	Venezuela	AT&T +800 998 2112
Dominican Republic	AT&T +800 998 2112	Virgin Islands	57 1 657 0888

You can also obtain support in this region in the following ways:

- Spanish speakers, enter the URL: <http://lat.3com.com/lat/support/form.html>
- Portuguese speakers, enter the URL: <http://lat.3com.com/br/support/form.html>
- English speakers in Latin America, send e-mail to: lat_support_anc@3com.com

Country	Telephone Number	Country	Telephone Number
US and Canada — Telephone Technical Support and Repair			
All locations:	Network Jacks; Wired or Wireless Network Interface Cards:		1 847-262-0070
	All other 3Com products:		1 800 876 3266

INDEX

A

autoboot 722

B

backup 664

boot 723

C

change 725

clear accounting 213

clear ap 70

clear ap boot-configuration 310

clear ap local-switching vlan-profile 307

clear ap radio 308

clear authentication admin 214

clear authentication console 215

clear authentication dot1x 216

clear authentication mac 217

clear authentication proxy 218

clear banner motd 42

clear boot backup-configuration 666

clear boot config 666

clear dot1x bonded-period 594

clear dot1x max-req 595

clear dot1x port-control 595

clear dot1x quiet-period 596

clear dot1x reauth-max 597

clear dot1x reauth-period 597

clear dot1x timeout auth-server 598

clear dot1x timeout supplicant 598

clear dot1x tx-period 599

clear fdb 104

clear history 43

clear igmp statistics 514

clear interface 137

clear ip alias 138

clear ip dns domain 139

clear ip dns server 139

clear ip route 140

clear ip telnet 141

clear location policy 219

clear log 711

clear log buffer 711

clear log server 711

clear log trace 692

clear mac-user 220

clear mac-user attr 221

clear mac-user group 221

clear mac-usergroup 222

clear mac-usergroup attr 223

clear mobility-domain 280

clear mobility-domain member 280

clear mobility-profile 224

clear network-domain 292

clear network-domain mode 293

clear network-domain peer 294

clear network-domain seed-ip 295

clear ntp server 141

clear ntp update-interval 142

clear port counters 71

clear port media-type 72

clear port mirror 73

clear port name 72

clear port type 74

clear port-group 71

clear qos 129

clear radio-profile 312

clear radius 578

clear radius client system-ip 579

clear radius server 581

clear rfdetect attack-list 630

clear rfdetect black-list 631

clear rfdetect ignore 631

clear rfdetect ssid-list 632

clear rfdetect vendor-list 633

clear security 12-restrict 105

clear security 12-restrict counters 106

clear security acl 538

clear security acl map 539

clear server group 581

clear server group load-balance 581

clear service-profile 313

clear sessions 613

clear sessions network 615

clear snmp community 143

clear snmp notify profile 143
 clear snmp notify target 144
 clear snoop 700
 clear snoop map 700
 clear spantree portcost 484
 clear spantree portpri 485
 clear spantree portvlancost 485
 clear spantree portvlanpri 486
 clear spantree statistics 487
 clear summertime 145
 clear system 44
 clear system countrycode 44
 clear system ip-address 44, 146
 clear system location 44
 clear system name 44
 clear timezone 146
 clear trace 692
 clear user 224
 clear user attr 225
 clear user group 226
 clear user lockout 226
 clear usergroup 227
 clear usergroup attr 228
 clear vlan 107
 clear vlan-profile 108
 commit security acl 541
 copy 667
 create 726
 crypto certificate 564
 crypto certificate admin 564
 crypto certificate eap 564
 crypto generate key 565
 crypto generate request 566
 crypto generate request admin 566
 crypto generate request eap 566
 crypto generate self-signed 568
 crypto generate self-signed admin 568
 crypto generate self-signed eap 568
 crypto otp 570
 crypto otp admin 570
 crypto otp eap 570
 crypto pkcs12 572
 crypto pkcs12 admin 572
 crypto pkcs12 eap 572

D

delete 669, 727
 dhcp 728
 diag 729
 dir 670, 729
 disable 37
 display 730
 display aaa 229
 display accounting statistics 232
 display ap boot-configuration 342
 display ap config 314, 316, 481
 display ap connection 343
 display ap counters 319
 display ap etherstats 327
 display ap fdb 325
 display ap global 345
 display ap group 329
 display ap mesh-links 329
 display ap qos-stats 326
 display ap status 331
 display ap unconfigured 347
 display ap vlan 337
 display arp 147
 display auto-tune attributes 338
 display auto-tune neighbors 340
 display banner motd 45
 display base-information 45
 display boot 674
 display config 675
 display crypto ca-certificate 573
 display crypto certificate 574
 display crypto key domain 576
 display crypto key ssh 576
 display dhcp-client 148
 display dhcp-server 150
 display dot1x 599
 display fdb 109
 display fdb agingtime 111
 display fdb count 112
 display igmp 514
 display igmp mrouter 518
 display igmp querier 519
 display igmp receiver-table 521
 display igmp statistics 523
 display interface 152
 display ip alias 153
 display ip dns 154
 display ip https 155
 display ip route 156
 display ip telnet 158
 display license 46
 display load 47
 display load-balancing group 348
 display location policy 234
 display log buffer 712
 display log config 714
 display log trace 715
 display mobility-domain config 281, 282
 display mobility-domain status 283
 display mobility-profile 235

display network-domain 296
 display ntp 159
 display port counters 75
 display port media-type 81
 display port mirror 77
 display port poe 78
 display port status 79
 display port-group 76
 display qos 133
 display qos dscp-table 134
 display radio-profile 350
 display rfdetect attack-list 635
 display rfdetect black-list 636
 display rfdetect clients 637
 display rfdetect countermeasures 639
 display rfdetect counters 640
 display rfdetect data 642
 display rfdetect ignore 644
 display rfdetect mobility-domain 644
 display rfdetect ssid-list 649
 display rfdetect vendor-list 649
 display rfdetect visible 650
 display roaming station 113
 display roaming vlan 115
 display security 12-restrict 116
 display security acl 542
 display security acl editbuffer 542, 543
 display security acl hits 544
 display security acl info 545
 display security acl map 546
 display security acl resource-usage 547
 display service-profile 353
 display sessions 616, 619
 display sessions mesh-ap 619
 display sessions network 620
 display snmp community 161
 display snmp counters 162
 display snmp notify profile 162
 display snmp notify target 162
 display snmp status 163
 display snmp usm 164
 display snoop 706
 display snoop info 706
 display snoop map 707
 display snoop stats 708
 display spantree 488
 display spantree backbonefast 491
 display spantree blockedports 492
 display spantree portfast 493
 display spantree portvlancost 494
 display spantree statistics 494
 display spantree uplinkfast 500
 display summertime 164

display system 47
 display timedate 165
 display timezone 165
 display trace 693
 display tunnel 117
 display version 677
 display vlan config 118

E

et 658

F

fver 732

H

help 50, 733
 history 51

I

install soda agent 673

L

load config 679
 ls 734

M

md5 681
 mkdir 681
 monitor port counters 82

N

next 735

P

ping 166

Q

quickstart 52
 quit 38

R

reset 736
 reset ap 362

reset port 87
 reset system 683
 restore 684
 rfping 634
 rmdir 685
 rollback security acl 551

S

save config 685
 save trace 694
 set accounting {admin | console} 235
 set accounting {dot1x | mac | web | last-resort} 237
 set ap 87
 set ap auto 362
 set ap auto mode 366
 set ap auto persistent 364
 set ap auto radiotype 365
 set ap bias 367
 set ap blink 368, 379
 set ap boot-configuration mesh mode 370
 set ap boot-configuration mesh psk-phrase 371
 set ap boot-configuration mesh psk-raw 372
 set ap boot-configuration mesh ssid 373
 set ap boot-ip 369
 set ap boot-switch 374
 set ap boot-vlan 375
 set ap fingerprint 376
 set ap force-image-download 378
 set ap local-switching mode 379
 set ap local-switching vlan-profile 380
 set ap name 381
 set ap radio antenna-location 382
 set ap radio antennatype 383
 set ap radio auto-tune max-power 384
 set ap radio auto-tune max-retransmissions 385
 set ap radio channel 387
 set ap radio link-calibration 388
 set ap radio load balancing 389
 set ap radio load balancing group 390
 set ap radio mode 391
 set ap radio radio-profile 392
 set ap radio tx-power 393
 set ap security 395
 set ap upgrade-firmware 396, 398
 set arp 168
 set arp agingtime 169
 set authentication admin 239
 set authentication console 241
 set authentication dot1x 243
 set authentication mac 247
 set authentication max-attempts 249, 250
 set authentication minimum-password-length 251
 set authentication password-restrict 252

set authentication proxy 253
 set authentication web 254
 set auto-config 52
 set band-preference 397
 set banner acknowledge 54
 set banner motd 56
 set boot backup-configuration 686
 set boot backup-configuration 686
 set boot configuration-file 687, 688
 set confirm 57
 set domain security 289
 set dot1x authcontrol 602
 set dot1x bonded-period 603
 set dot1x key-tx 604
 set dot1x max-req 605
 set dot1x port-control 606
 set dot1x quiet-period 607
 set dot1x reauth 607
 set dot1x reauth-max 608
 set dot1x reauth-period 609
 set dot1x timeout auth-server 609
 set dot1x timeout supplicant 610
 set dot1x tx-period 610
 set dot1x wep-rekey 611
 set dot1x wep-rekey-period 612
 set enablepass 39
 set fdb 121
 set fdb agingtime 122
 set igmp 525
 set igmp mrouter 527
 set igmp mrsol 528
 set igmp mrsol mrsi 528
 set igmp oqi 529
 set igmp proxy-report 530
 set igmp qi 531
 set igmp qri 532
 set igmp querier 533
 set igmp receiver 533
 set igmp rv 534
 set interface 170
 set interface dhcp-server 172
 set interface status 173
 set ip alias 174
 set ip dns 175
 set ip dns domain 175
 set ip dns server 176
 set ip https server 177
 set ip route 178
 set ip snmp server 180
 set ip ssh 180
 set ip ssh server 181
 set ip telnet 181
 set ip telnet server 182
 set length 57

- set license 58
- set load-balancing strictness 399
- set location policy 256
- set log 716
- set log buffer 716
- set log console 716
- set log current 716
- set log mark 719
- set log server 716
- set log sessions 716
- set log trace 716
- set mac-user 260
- set mac-user attr 261
- set mac-usergroup attr 267
- set mobility profile 269
- set mobility-domain member 284
- set mobility-domain mode member seed-ip 285, 286
- set mobility-domain mode secondary-seed domain-name 287
- set mobility-domain mode seed domain-name 288
- set mobility-profile mode 271
- set network-domain mode member seed-ip 298
- set network-domain mode seed domain-name 300
- set network-domain peer 299
- set ntp 183
- set ntp server 184
- set ntp update-interval 185
- set port 89
- set port media-type 91
- set port mirror 92
- set port name 93
- set port negotiation 93
- set port poe 94
- set port speed 95
- set port trap 96
- set port type ap 97
- set port type wired-auth 100
- set port-group 90
- set prompt 59
- set qos cos-to-dscp-map 131
- set qos dscp-to-cos-map 132
- set radio-profile active-scan 400
- set radio-profile auto-tune channel-config 402
- set radio-profile auto-tune channel-holddown 403
- set radio-profile auto-tune channel-interval 404
- set radio-profile auto-tune channel-lockdown 405
- set radio-profile auto-tune power-config 406
- set radio-profile auto-tune power-interval 407
- set radio-profile beacon-interval 400, 409
- set radio-profile countermeasures 410
- set radio-profile dtim-interval 412
- set radio-profile frag-threshold 413
- set radio-profile long-retry 414
- set radio-profile max-rx-lifetime 414
- set radio-profile max-tx-lifetime 415
- set radio-profile mode 416
- set radio-profile preamble-length 419
- set radio-profile qos-mode 420
- set radio-profile rfid-mode 421
- set radio-profile rts-threshold 421, 423
- set radio-profile service-profile 424
- set radio-profile short-retry 430
- set radio-profile wmm 430
- set radio-profile wmm-powersave 430
- set radius 582
- set radius client system-ip 584
- set radius deadline 582
- set radius key 582
- set radius proxy client 585
- set radius proxy port 586
- set radius retransmit 582
- set radius server 587
- set radius timeout 582
- set refetect ssid-list 659
- set rfdetect active-scan 652
- set rfdetect attack-list 653
- set rfdetect black-list 654
- set rfdetect countermeasures 654
- set rfdetect countermeasures mac 655
- set rfdetect ignore 656
- set rfdetect log 657
- set rfdetect signature 658
- set rfdetect signature key 659
- set rfdetect vendor-list 660
- set security 12-restrict 123
- set security acl 552
- set security acl hit-sample-rate 559
- set security acl ip icmp 552
- set security acl ip ip 552
- set security acl ip tcp 552
- set security acl ip udp 552
- set security acl map 557
- set server group 589
- set server group load-balance 590
- set service-profile attr 431
- set service-profile auth-dot1x 433
- set service-profile auth-fallthru 434
- set service-profile auth-psk 435
- set service-profile beacon 436
- set service-profile bridging 437
- set service-profile cac-mode 438
- set service-profile cac-session 439
- set service-profile cipher-ccmp 440
- set service-profile cipher-tkip 441
- set service-profile cipher-wep104 442
- set service-profile cipher-wep40 443

set service-profile cos 444
 set service-profile dhcp-restrict 445
 set service-profile idle-client-probing 446
 set service-profile keep-initial-vlan 447
 set service-profile load-balancing- 448
 set service-profile long-retry-count 449
 set service-profile no-broadcast 451
 set service-profile proxy-arp 452
 set service-profile psk-phrase 453
 set service-profile psk-raw 454
 set service-profile rsn-ie 455
 set service-profile shared-key-auth 456
 set service-profile short-retry-count 456
 set service-profile soda agent-directory 457
 set service-profile soda enforce-checks 458
 set service-profile soda failure-page 459
 set service-profile soda logout-page 460
 set service-profile soda mode 462
 set service-profile soda remediation-acl 463
 set service-profile soda success-page 464
 set service-profile ssid-name 465
 set service-profile ssid-type 466
 set service-profile static-cos 467
 set service-profile tkip-mc-time 466
 set service-profile transmit-rates 468
 set service-profile use-client-dscp 470
 set service-profile user-idle-timeout 471
 set service-profile web-auth-url 473, 475, 476
 set service-profile web-portal-acl 472
 set service-profile web-portal-session-timeout 477
 set service-profile wep active-multicast-index 478
 set service-profile wep active-unicast-index 479
 set service-profile wep key-index 480
 set service-profile wpa-ie 481
 set snmp community 185
 set snmp notify profile 187
 set snmp notify target 192
 set snmp protocol 197
 set snmp security 198
 set snmp usm 199
 set snoop 701
 set snoop map 704
 set snoop mode 705
 set spantree 501
 set spantree backbonefast 502
 set spantree fwddelay 503
 set spantree hello 503
 set spantree maxage 504
 set spantree portcost 505
 set spantree portfast 506
 set spantree portpri 507
 set spantree portvlancost 508
 set spantree portvlanpri 509
 set spantree priority 510

set spantree uplinkfast 510
 set summertime 202
 set system contact 60
 set system countrycode 61
 set system idle-timeout 65
 set system ip-address 66, 203
 set system location 67
 set system name 68
 set timedate 204
 set timezone 205
 set trace authentication 694
 set trace authentication mac-addr 694
 set trace authentication port 694
 set trace authentication user 694
 set trace authorization 695
 set trace authorization mac-addr 695
 set trace authorization port 695
 set trace authorization user 695
 set trace dot1x 696
 set trace dot1x mac-addr 696
 set trace dot1x port 696
 set trace dot1x user 696
 set trace sm 697
 set trace sm mac-addr 697
 set trace sm port 697
 set trace sm user 697
 set user 271
 set user attr 273
 set user expire-password-in 274
 set user group 275
 set user password 271
 set usergroup 275
 set usergroup attr 275
 set usergroup expire-password-in 277
 set vlan name 124
 set vlan port 125
 set vlan profile 127
 set vlan tunnel-affinity 126
 set web-portal 278

T

telnet 206
 test 737
 test rflink 661
 traceroute 207

U

uninstall soda agent 688

V

version 738